



US011924213B2

(12) **United States Patent**
Felice-Steele et al.

(10) **Patent No.:** **US 11,924,213 B2**
(45) **Date of Patent:** ***Mar. 5, 2024**

(54) **USER PERMISSIONS FOR ACCESS TO SECURE DATA AT THIRD-PARTY**

Related U.S. Application Data

(71) Applicant: **ConsumerInfo.com, Inc.**, Costa Mesa, CA (US)

(63) Continuation of application No. 16/445,808, filed on Jun. 19, 2019, now Pat. No. 11,265,324.
(Continued)

(72) Inventors: **Michelle Felice-Steele**, Woodland Hills, CA (US); **Michele Raneri**, Orange, CA (US); **Paul DeSaulniers**, Ladera Ranch, CA (US); **Joe Manna**, Tustin, CA (US); **Jeff Softley**, Rancho Mission Viejo, CA (US); **Srikumar Puthupadi Kanthadai**, El Monte, CA (US); **Aga Dzhafar Hady Ogiu Dzhafarov**, Mission Viejo, CA (US); **Pat Finneran**, Queen Creek, AZ (US); **Donna Meryl Smith**, Irvine, CA (US); **Gregory Lennox Wright**, Newport Coast, CA (US); **Marizette Galvez**, Chino, CA (US); **Ujjayan Banerjee**, Irvine, CA (US); **Ravi Devesetti**, Fremont, CA (US); **Shivakumar Ramanathan**, Irvine, CA (US); **Mukeshkumar G. Patel**, Downey, CA (US)

(51) **Int. Cl.**
H04L 9/40 (2022.01)
G06F 9/451 (2018.01)
(Continued)

(52) **U.S. Cl.**
CPC **H04L 63/102** (2013.01); **G06F 9/451** (2018.02); **G06F 9/54** (2013.01); **G06F 16/13** (2019.01);
(Continued)

(58) **Field of Classification Search**
CPC ... H04L 63/102; H04L 63/062; H04L 63/083; H04L 63/0861; H04L 63/0884;
(Continued)

(73) Assignee: **ConsumerInfo.com, Inc.**, Costa Mesa, CA (US)

(56) **References Cited**
U.S. PATENT DOCUMENTS
5,933,837 A 8/1999 Kung
6,477,509 B1 11/2002 Hammons et al.
(Continued)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

FOREIGN PATENT DOCUMENTS
BR 112013017973-2 10/2020
CA 2 509 842 12/2005
(Continued)

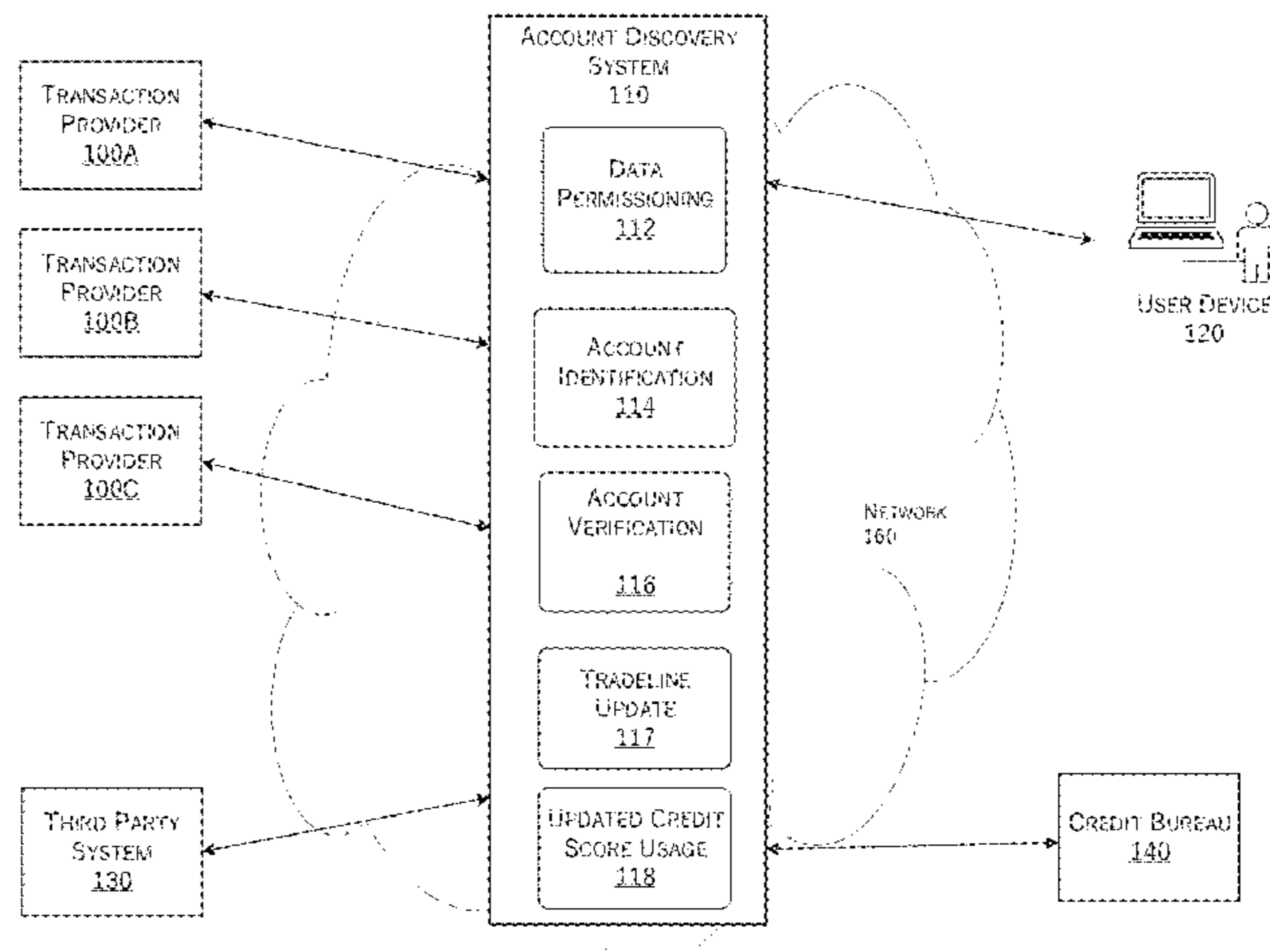
(21) Appl. No.: **17/578,238**

OTHER PUBLICATIONS
Solapurkar "Building Secure Healthcare Services Using OAuth 2.0 and JSON Web Token in IOT Cloud Scenario", IEEE, 2016, p. 99-104 (Year: 2016).*
(Continued)

(22) Filed: **Jan. 18, 2022**

(65) **Prior Publication Data**
US 2022/0217146 A1 Jul. 7, 2022

Primary Examiner — Catherine Thiaw
(74) *Attorney, Agent, or Firm* — Knobbe, Martens, Olson & Bear, LLP



(57) **ABSTRACT**

A user permission system manages and regulates access to secure data at one or more third-party data sites. The system may provide access to one or more databases or other data structures based on user authentication and access rules that have been established, such as by a user associated with the data being accessed at the third party data store. Access may be provided via an API to the third-party data site, along with access credentials of a user with data stored with the third-party data site, allowing the system to access data on behalf of the user.

20 Claims, 44 Drawing Sheets

Related U.S. Application Data

(60) Provisional application No. 62/826,319, filed on Mar. 29, 2019, provisional application No. 62/727,479, filed on Sep. 5, 2018.

(51) **Int. Cl.**

G06F 9/54 (2006.01)
G06F 16/13 (2019.01)
G06F 16/23 (2019.01)
G06F 16/245 (2019.01)
G06F 16/248 (2019.01)
G06F 21/62 (2013.01)
G06Q 40/03 (2023.01)
H04L 67/306 (2022.01)

(52) **U.S. Cl.**

CPC **G06F 16/23** (2019.01); **G06F 16/2379** (2019.01); **G06F 16/245** (2019.01); **G06F 16/248** (2019.01); **G06F 21/6218** (2013.01); **G06Q 40/03** (2023.01); **H04L 63/062** (2013.01); **H04L 63/083** (2013.01); **H04L 63/0861** (2013.01); **H04L 63/0884** (2013.01); **H04L 63/18** (2013.01); **H04L 67/306** (2013.01); **H04L 2463/121** (2013.01)

(58) **Field of Classification Search**

CPC . H04L 63/18; H04L 67/306; H04L 2463/121; G06F 9/451; G06F 16/2379; G06F 16/245; G06F 16/23; G06F 16/13; G06F 16/248; G06F 9/54; G06F 21/6218; G06Q 40/03

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,556,979 B1 4/2003 Liu et al.
 6,850,918 B1 2/2005 Burchetta et al.
 6,954,741 B1 10/2005 Burchetta et al.
 7,047,258 B2 5/2006 Balogh et al.
 7,249,096 B1 7/2007 Lasater et al.
 7,366,495 B1 4/2008 Magnotta et al.
 8,019,066 B1 9/2011 Efrati et al.
 8,165,962 B1 4/2012 LeKachman
 8,490,197 B2 7/2013 Herz
 8,712,789 B2 4/2014 Stibel et al.
 8,712,907 B1 4/2014 Stibel et al.
 8,713,651 B1 4/2014 Stibel
 8,725,605 B1 5/2014 Plunkett
 8,732,803 B2 5/2014 Stibel et al.
 8,930,383 B2 1/2015 Dekker et al.
 8,996,391 B2 3/2015 Stibel et al.
 9,092,616 B2 7/2015 Kumar et al.

9,111,281 B2 8/2015 Stibel et al.
 9,348,896 B2 5/2016 Faith et al.
 9,613,382 B1 4/2017 Newstadt et al.
 9,652,802 B1 5/2017 Kasower
 9,704,107 B1 7/2017 Baker, IV et al.
 9,824,199 B2 11/2017 Kshirsagar et al.
 10,002,075 B1 6/2018 O'Leary et al.
 10,798,113 B2 10/2020 Muddu et al.
 10,839,446 B1 11/2020 Mupkala et al.
 11,238,656 B1 2/2022 Lin et al.
 11,265,324 B2 3/2022 Felice-Steele et al.
 11,308,551 B1 4/2022 Mahacek et al.
 11,315,179 B1 4/2022 Rehder et al.
 11,347,715 B2 5/2022 Girulat, Jr.
 11,356,430 B1 6/2022 Kapczynski et al.
 11,373,109 B2 6/2022 Zoldi et al.
 11,373,261 B1 6/2022 Ramos et al.
 11,379,916 B1 7/2022 Taylor et al.
 11,399,029 B2 7/2022 Manna et al.
 11,410,230 B1 8/2022 Olson et al.
 11,425,144 B2 8/2022 Bondugula et al.
 11,436,626 B2 9/2022 Lawrence et al.
 11,461,364 B1 10/2022 Charyk et al.
 11,489,834 B1 11/2022 Carroll et al.
 11,514,519 B1 11/2022 Hunt, III
 11,562,457 B2 1/2023 Ramos et al.
 11,580,598 B1 2/2023 Rehder et al.
 11,631,130 B1 4/2023 Taylor et al.
 2001/0047307 A1 11/2001 Bennett et al.
 2002/0072975 A1 6/2002 Steele et al.
 2003/0033231 A1 2/2003 Turner et al.
 2003/0041021 A1 2/2003 Kogler et al.
 2003/0088472 A1 5/2003 Offutt et al.
 2003/0144907 A1 7/2003 Cohen, Jr. et al.
 2003/0144933 A1 7/2003 Huang
 2003/0225729 A1 12/2003 Maloche et al.
 2004/0107161 A1 6/2004 Tanaka et al.
 2004/0133460 A1 7/2004 Berlin et al.
 2004/0138935 A1 7/2004 Johnson et al.
 2004/0249789 A1 12/2004 Kapoor et al.
 2005/0027817 A1 2/2005 Novik et al.
 2007/0203954 A1 8/2007 Vargas et al.
 2007/0276780 A1 11/2007 Iriyama et al.
 2007/0299772 A1 12/2007 Mastie et al.
 2008/0015954 A1 1/2008 Huber et al.
 2008/0115226 A1 5/2008 Welinkar et al.
 2008/0120155 A1 5/2008 Pliha
 2008/0120204 A1 5/2008 Conner et al.
 2008/0120416 A1 5/2008 Hopkins et al.
 2008/0120569 A1 5/2008 Mann et al.
 2008/0120716 A1 5/2008 Hall et al.
 2008/0122920 A1 5/2008 Chang
 2008/0126136 A1 5/2008 Nighan
 2008/0126233 A1 5/2008 Hogan
 2008/0133273 A1 6/2008 Marshall
 2008/0133278 A1 6/2008 Stanfield
 2008/0133322 A1 6/2008 Kalia et al.
 2008/0133657 A1 6/2008 Pennington
 2008/0140476 A1 6/2008 Anand et al.
 2008/0140507 A1 6/2008 Hamlisch et al.
 2008/0140734 A1 6/2008 Wagner
 2008/0140780 A1 6/2008 Hopkins et al.
 2008/0141346 A1 6/2008 Kay et al.
 2008/0147523 A1 6/2008 Mulry et al.
 2008/0148368 A1 6/2008 Zurko et al.
 2008/0148392 A1 6/2008 Akens
 2008/0154758 A1 6/2008 Schattmaier et al.
 2008/0162236 A1 7/2008 Sommerer
 2008/0162317 A1 7/2008 Banaugh et al.
 2008/0162350 A1 7/2008 Allen-Rouman et al.
 2008/0162383 A1 7/2008 Kraft
 2008/0172304 A1 7/2008 Berkowitz
 2008/0172324 A1 7/2008 Johnson
 2008/0175360 A1 7/2008 Schwarz et al.
 2009/0125439 A1 5/2009 Zarikian et al.
 2009/0132813 A1 5/2009 Schibuk
 2011/0047086 A1 2/2011 Heisterkamp et al.
 2011/0289094 A1 11/2011 Fisher
 2012/0036053 A1 2/2012 Miller

(56)

References Cited

U.S. PATENT DOCUMENTS

2012/0078766 A1 3/2012 Rose et al.
 2012/0239583 A1 9/2012 Dobrowolski
 2012/0246092 A1 9/2012 Stibel et al.
 2012/0246093 A1 9/2012 Stibel et al.
 2012/0278249 A1 11/2012 Duggal et al.
 2012/0290486 A1 11/2012 Dobrowolski et al.
 2012/0296804 A1 11/2012 Stibel et al.
 2012/0323695 A1 12/2012 Stibel
 2013/0007891 A1* 1/2013 Mogaki G06F 21/6218
 726/27
 2013/0013553 A1 1/2013 Stibel et al.
 2013/0024367 A1 1/2013 Bellefeuille et al.
 2013/0031105 A1 1/2013 Stibel et al.
 2013/0232018 A1 9/2013 Keithley et al.
 2013/0238387 A1 9/2013 Stibel et al.
 2013/0339141 A1 12/2013 Stibel et al.
 2014/0025562 A1 1/2014 Rothrock et al.
 2014/0095640 A1 4/2014 Stibel et al.
 2014/0114735 A1 4/2014 Isaacson et al.
 2014/0122354 A1 5/2014 Stibel et al.
 2014/0173732 A1 6/2014 Stibel
 2015/0142639 A1 5/2015 Padawer
 2015/0161228 A1 6/2015 Davies
 2015/0262249 A1 9/2015 Wical
 2015/0278277 A1 10/2015 Agrawal et al.
 2016/0070758 A1 3/2016 Thomson et al.
 2016/0232546 A1 8/2016 Ranft
 2017/0070500 A1 3/2017 Hockey et al.
 2017/0359346 A1* 12/2017 Parab H04L 67/02
 2018/0097828 A1 4/2018 Coskun
 2018/0176267 A1* 6/2018 Malatesha H04L 65/403
 2018/0285981 A1 10/2018 Andringa et al.
 2019/0019185 A1* 1/2019 Chitalia G06Q 20/383
 2019/0102438 A1 4/2019 Murray et al.
 2019/0147366 A1 5/2019 Sankaran et al.
 2020/0120004 A1 4/2020 Kohout et al.
 2020/0126126 A1 4/2020 Briancon et al.
 2020/0137110 A1 4/2020 Tyler et al.
 2020/0210466 A1 7/2020 Yin et al.
 2020/0349639 A1 11/2020 Mousseau
 2021/0027357 A1 1/2021 Bonfigli et al.
 2021/0152567 A1 5/2021 Huston, III et al.
 2021/0194885 A1 6/2021 Manna
 2021/0234869 A1 7/2021 Bondugula et al.
 2022/0027853 A1 1/2022 McMillan et al.
 2022/0051315 A1 2/2022 Robida et al.
 2022/0327653 A1 10/2022 Ramos et al.
 2022/0335032 A1 10/2022 Girulat, Jr.
 2022/0374744 A1 11/2022 Zoldi et al.
 2023/0007007 A1 1/2023 Manna
 2023/0054085 A1 2/2023 Bondugula et al.

FOREIGN PATENT DOCUMENTS

CA 2 611 595 12/2006
 CN 1290373 4/2001
 EP 0 350 907 1/1990
 EP 0 468 440 1/1992
 EP 0 542 298 5/1993
 EP 0 566 736 8/1993
 EP 0 869 652 10/1998
 EP 0 913 789 5/1999
 EP 0 919 942 6/1999
 EP 1 028 401 8/2000
 EP 1 239 378 9/2002
 EP 1 301 887 4/2003
 EP 1 550 960 7/2005
 EP 1 591 931 11/2005
 EP 1 850 278 10/2007
 EP 2 088 743 8/2009
 EP 2 151 793 2/2010
 EP 2 472 423 7/2012
 GB 2 102 606 2/1983

WO WO 00/052616 9/2000
 WO WO 01/045012 6/2001
 WO WO 2012/054401 4/2012

OTHER PUBLICATIONS

Gustafsson E, Jonsson A. Always best connected. IEEE Wireless communications. Feb. 28, 2003;10(1):49-55 (Year: 2003).*
 U.S. Appl. No. 16/445,808, 2020/0076813, User Permissions for Access to Secure Data at Third-Party, filed Jun. 19, 2019.
 Provisional Application as filed in U.S. Appl. No. 60/168,272, dated Dec. 1, 1999 in 14 pages.
 Provisional Application as filed in U.S. Appl. No. 60/168,276, dated Dec. 1, 1999 in 82 pages.
 Provisional Application as filed in U.S. Appl. No. 60/213,367, dated Jun. 23, 2000 in 20 pages.
 Application as filed in U.S. Appl. No. 09/411,683, dated Oct. 4, 1999.
 Application as filed in U.S. Appl. No. 09/653,595, dated Aug. 31, 2000.
 Application as filed in U.S. Appl. No. 09/790,453, dated Feb. 22, 2001.
 Office Action in U.S. Appl. No. 09/790,453, dated Jan. 20, 2006.
 Office Action in U.S. Appl. No. 09/790,453, dated Jul. 11, 2006.
 Office Action in U.S. Appl. No. 09/790,453, dated Dec. 1, 2006.
 Office Action in U.S. Appl. No. 09/790,453, dated May 10, 2007.
 Office Action in U.S. Appl. No. 09/790,453, dated Mar. 21, 2008.
 Application as filed in U.S. Appl. No. 10/183,135, filed Jun. 25, 2002.
 Office Action in U.S. Appl. No. 10/183,135, dated Oct. 22, 2007.
 Final Office Action in U.S. Appl. No. 10/183,135, dated Apr. 14, 2008.
 Office Action in U.S. Appl. No. 10/183,135, dated Aug. 21, 2008.
 Office Action in U.S. Appl. No. 10/183,135, dated Feb. 26, 2009.
 Office Action in U.S. Appl. No. 10/183,135, dated Aug. 18, 2009.
 Office Action in U.S. Appl. No. 10/183,135, dated Feb. 19, 2010.
 Final Office Action in U.S. Appl. No. 10/183,135, dated Sep. 22, 2010.
 Office Action in U.S. Appl. No. 10/183,135, dated Mar. 25, 2011.
 Notice of Allowance in U.S. Appl. No. 10/183,135, dated Aug. 15, 2011.
 Office Action in U.S. Appl. No. 11/169,769, dated Mar. 24, 2010.
 Application as Filed in U.S. Appl. No. 11/363,984, dated Feb. 27, 2006.
 Office Action in U.S. Appl. No. 11/363,984, dated Dec. 26, 2008.
 Caldeira et al., "Characterizing and Preventing Chargebacks in Next Generation Web Payments Services", 2012 Fourth International Conference on Computational Aspects of Social Networks (CASoN), 2012 IEEE, pp. 333-338.
 Delamaire et al., "Credit Card Fraud and Detection Techniques: A Review", Banks and Bank Systems, vol. 4, No. 2, 2009, pp. 57-68.
 European Network and Information Security Agency (enisa): Privacy and Security Risks when Authenticating on the Internet with European eID Cards, Nov. 2009, pp. 1-41.
 Federal Bureau of Investigation (FBI): The Cyber Threat to The Financial Sector: Testimony, Sep. 14, 2011, pp. 1-6.
 Hu et al. "Forecasting Identity Theft Victims: Analyzing Characteristics and Preventive Actions through Machine Learning Approaches", Victims & Offenders, 2021, vol. 16, No. 4, pp. 465-494.
 Peng et al., "Factors Affecting Online Purchase Behavior: Implications to Improve the Existing Credit Rating System", 2009 International Conference on Management and Service Science, 2009 IEEE, pp. 1-4.
 Poon, Martha Ann, "What Lenders See—A History of the Fair Isaac Scorecard", UCSD, ProQuest Dissertations Publishing, 2012, pp. 5. [Abstract Only].
 Skanderson, David M., "Managing Discrimination Risk of Machine Learning and AI Models", ABA Journal of Labor & Employment Law, 2021, pp. 339-360.

* cited by examiner

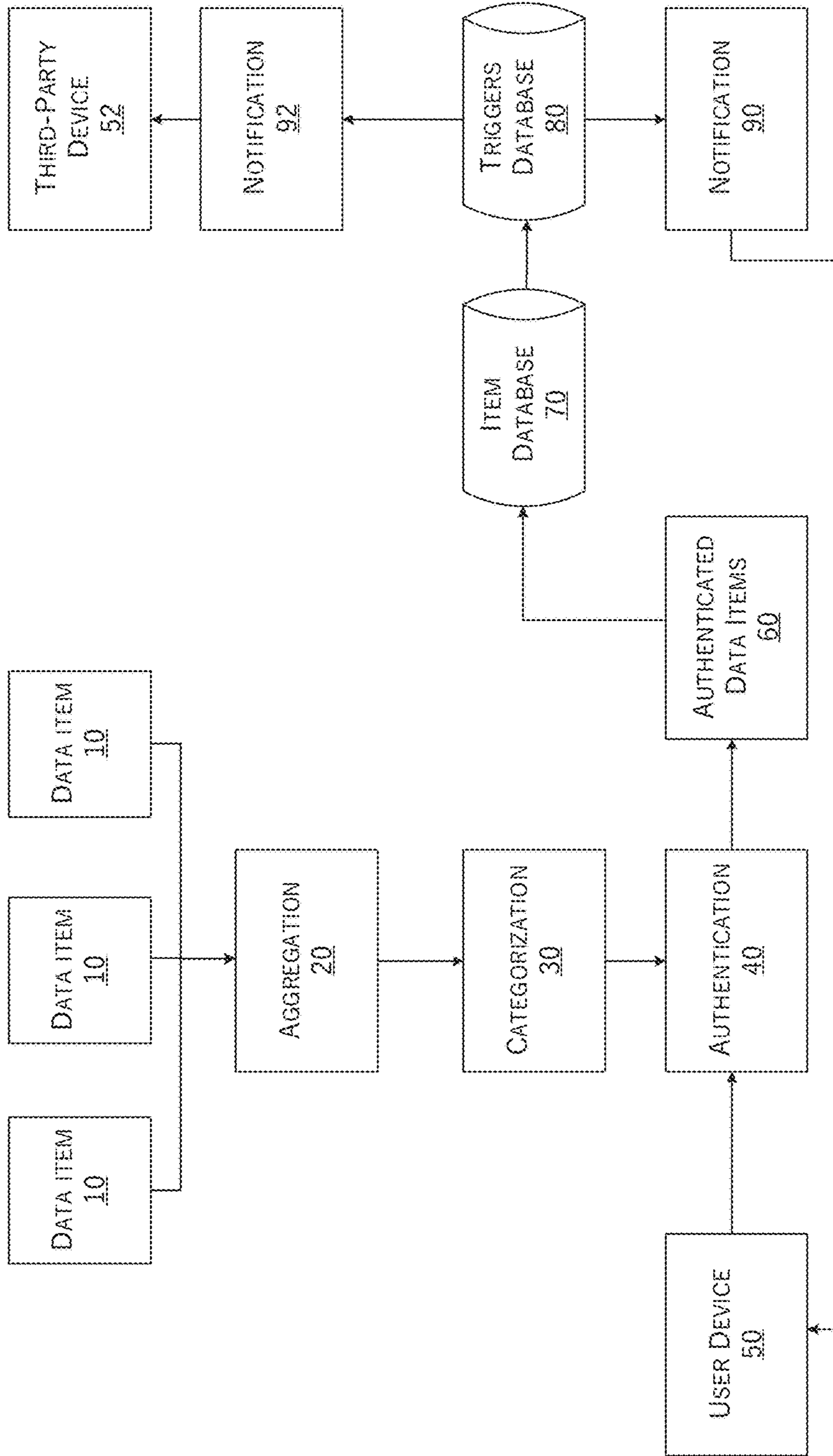


FIGURE 1

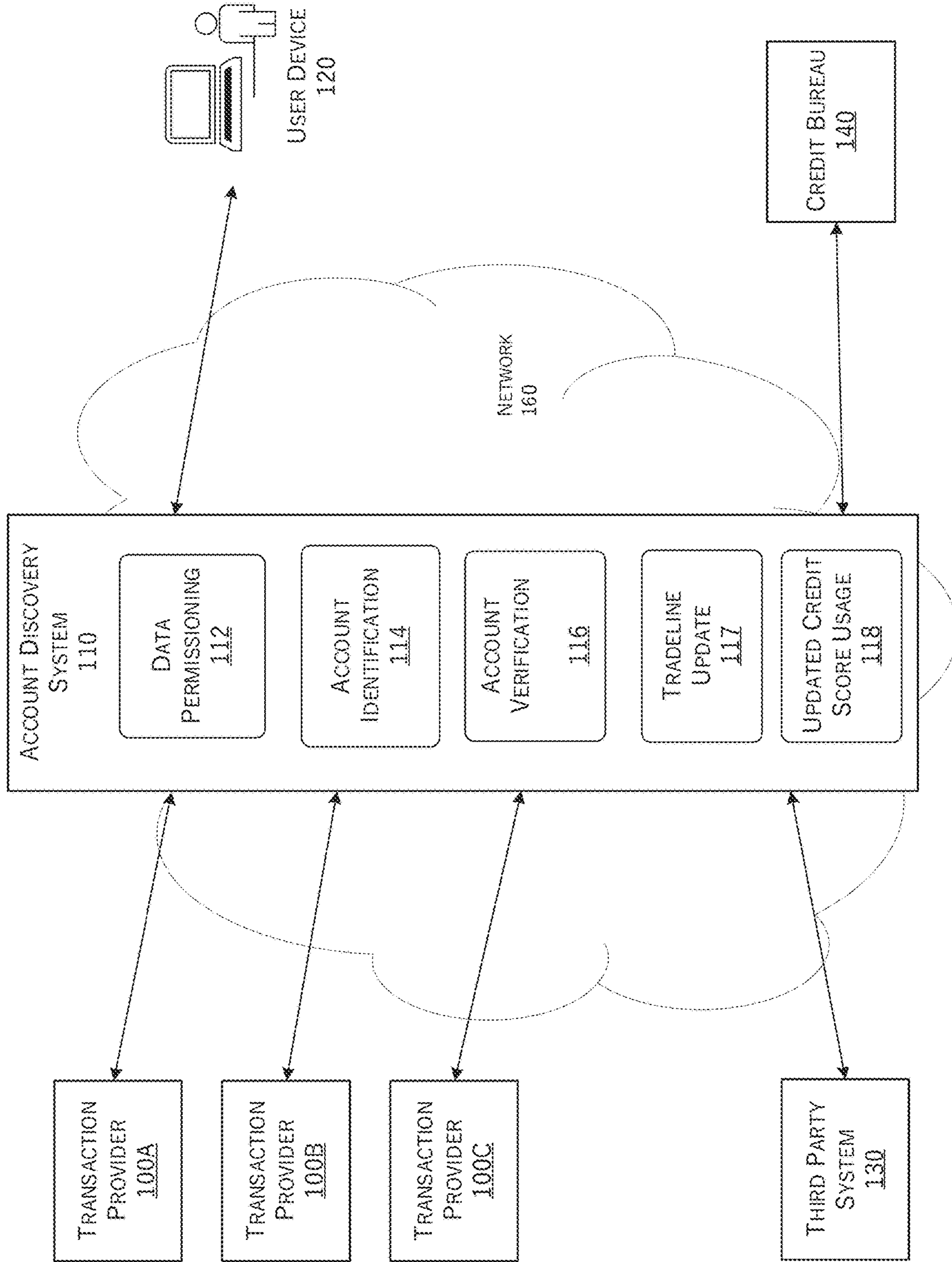


FIGURE 2A

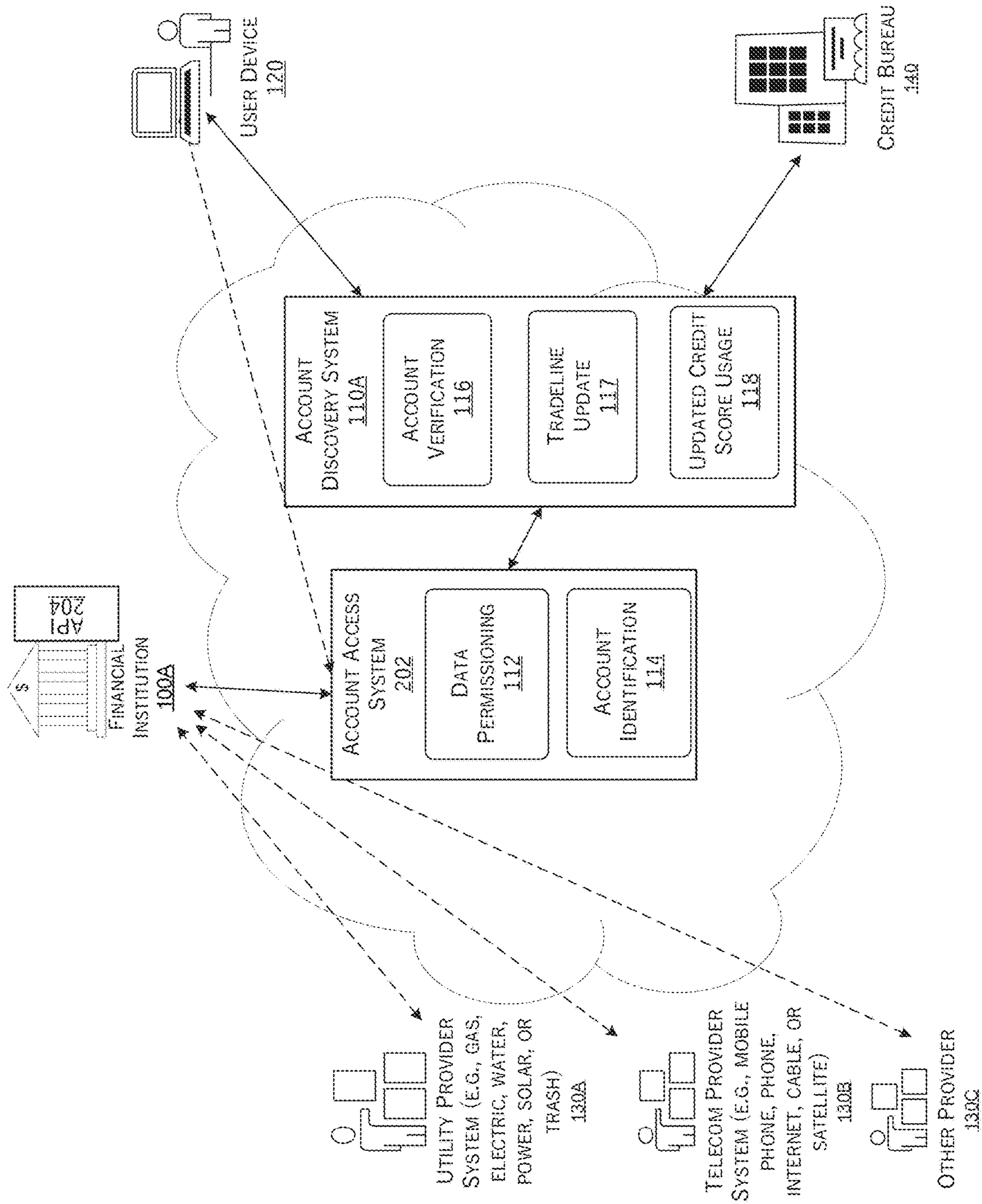


FIGURE 2B

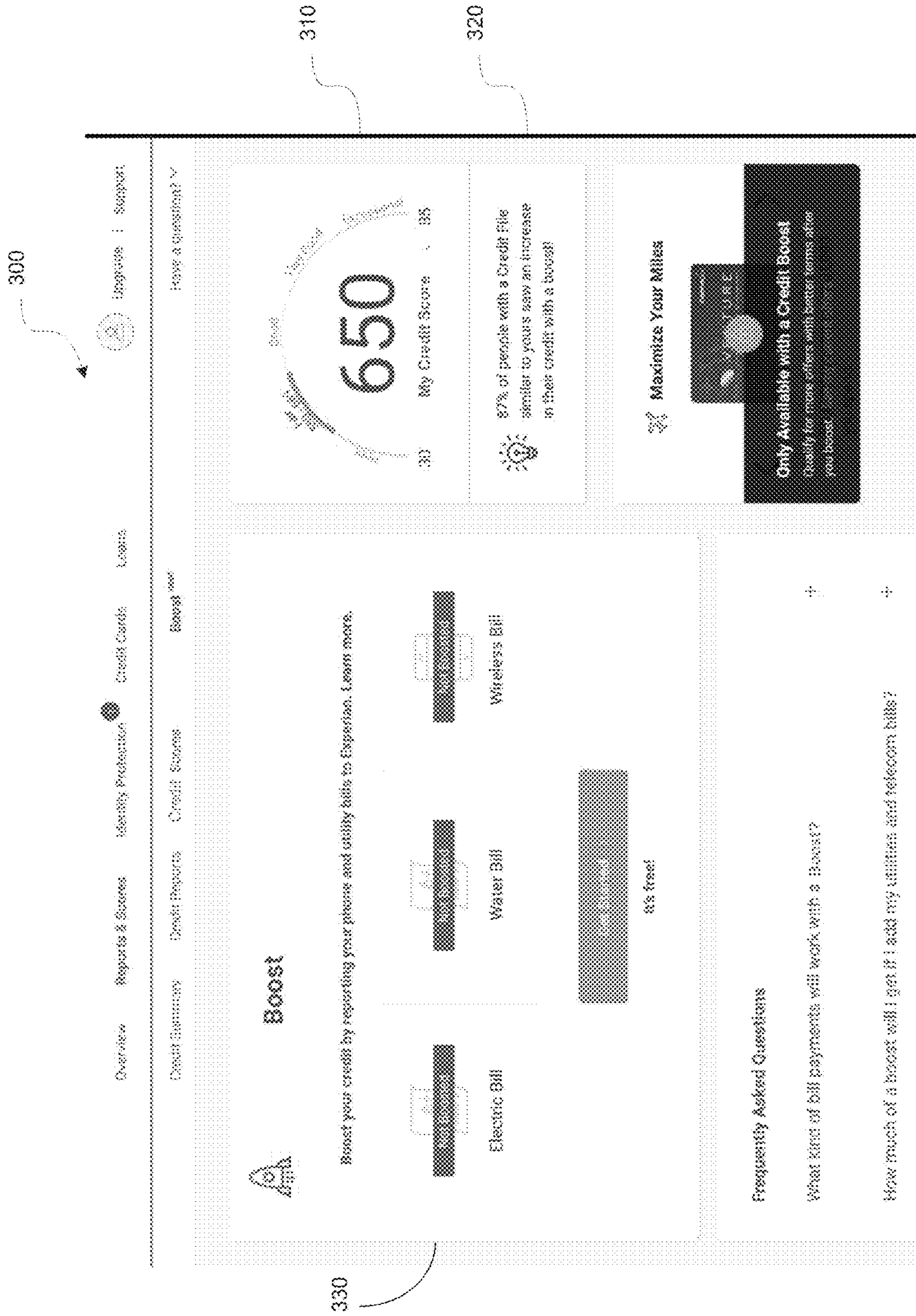


FIGURE 3

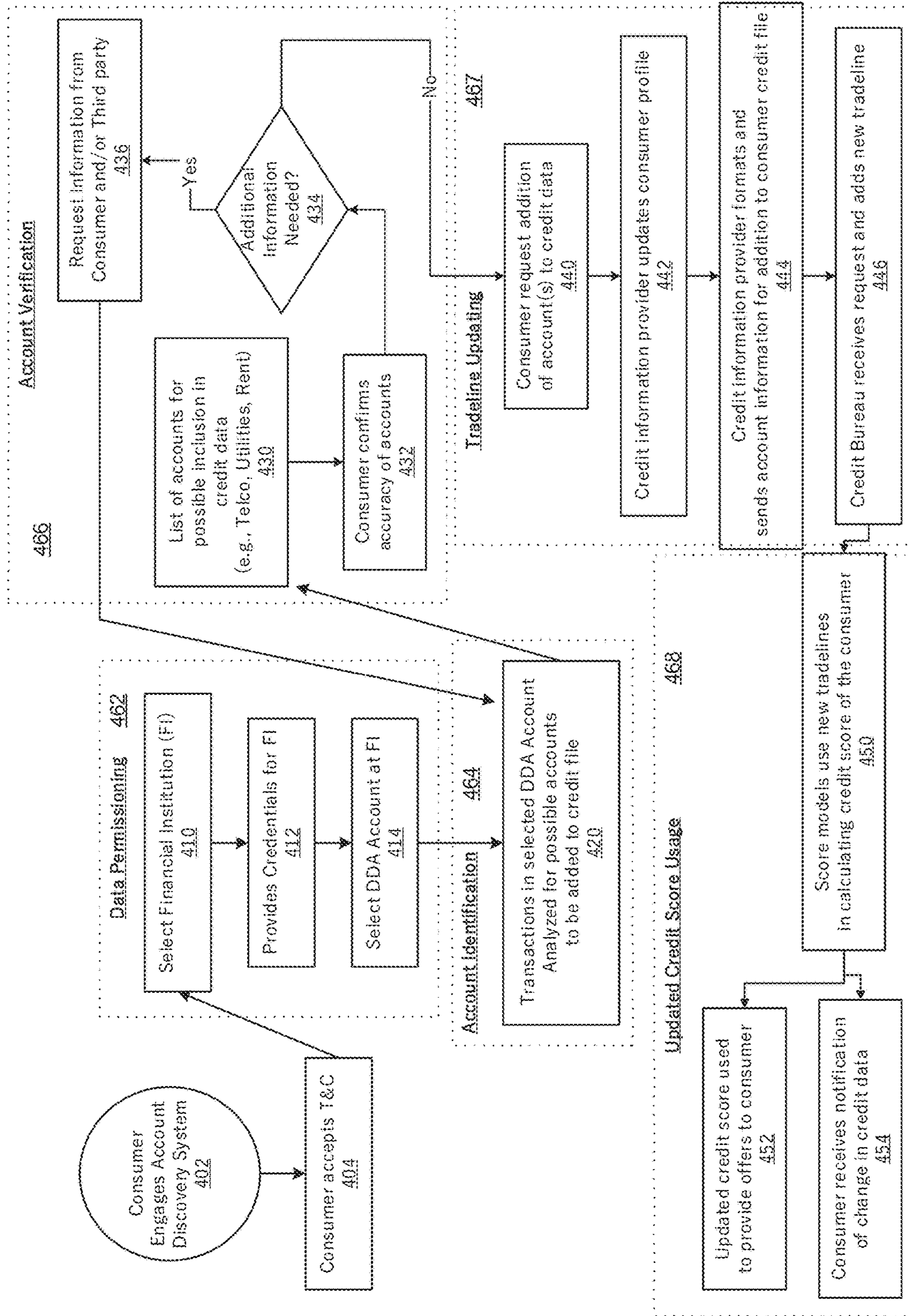


FIGURE 4

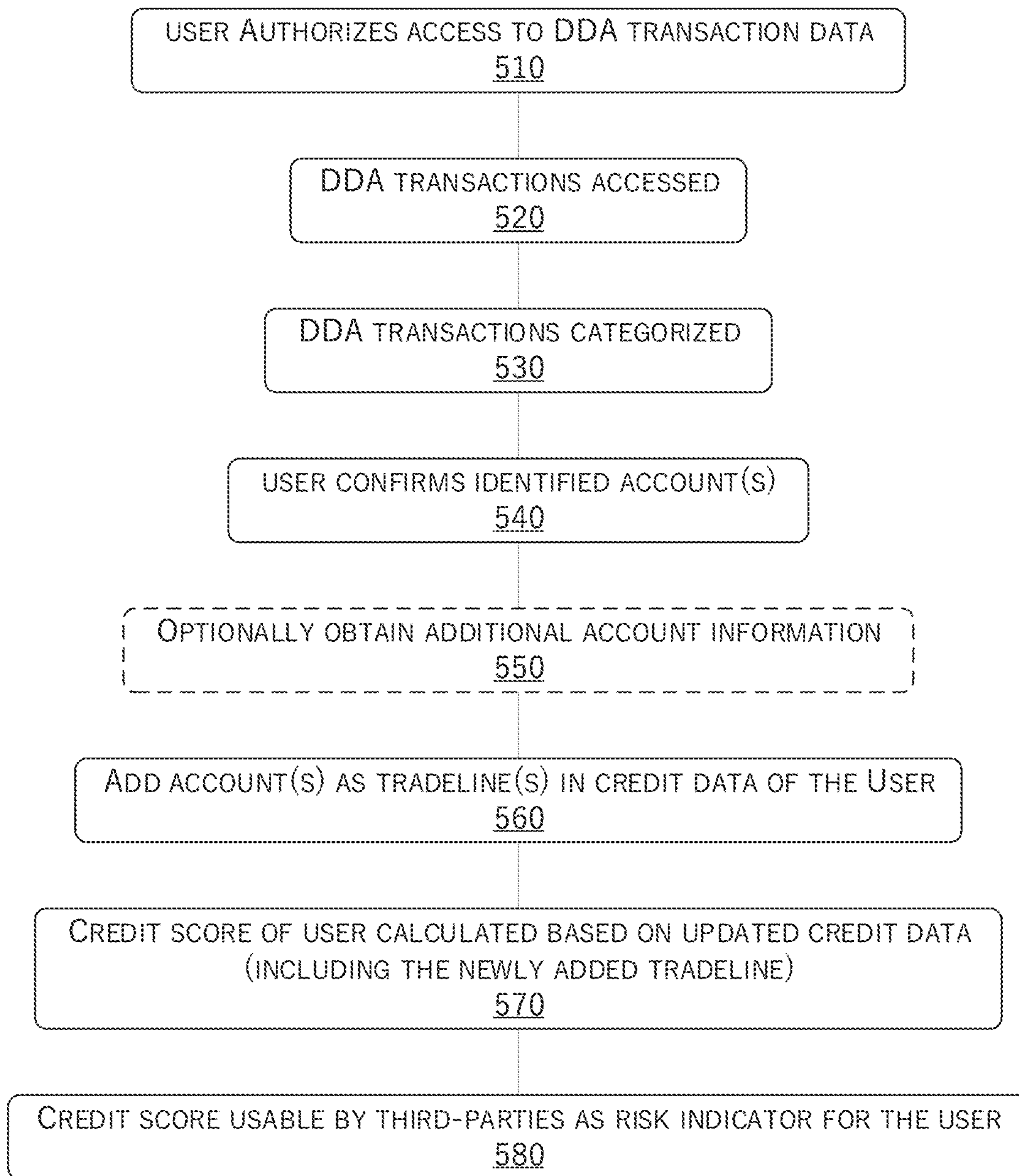


FIGURE 5

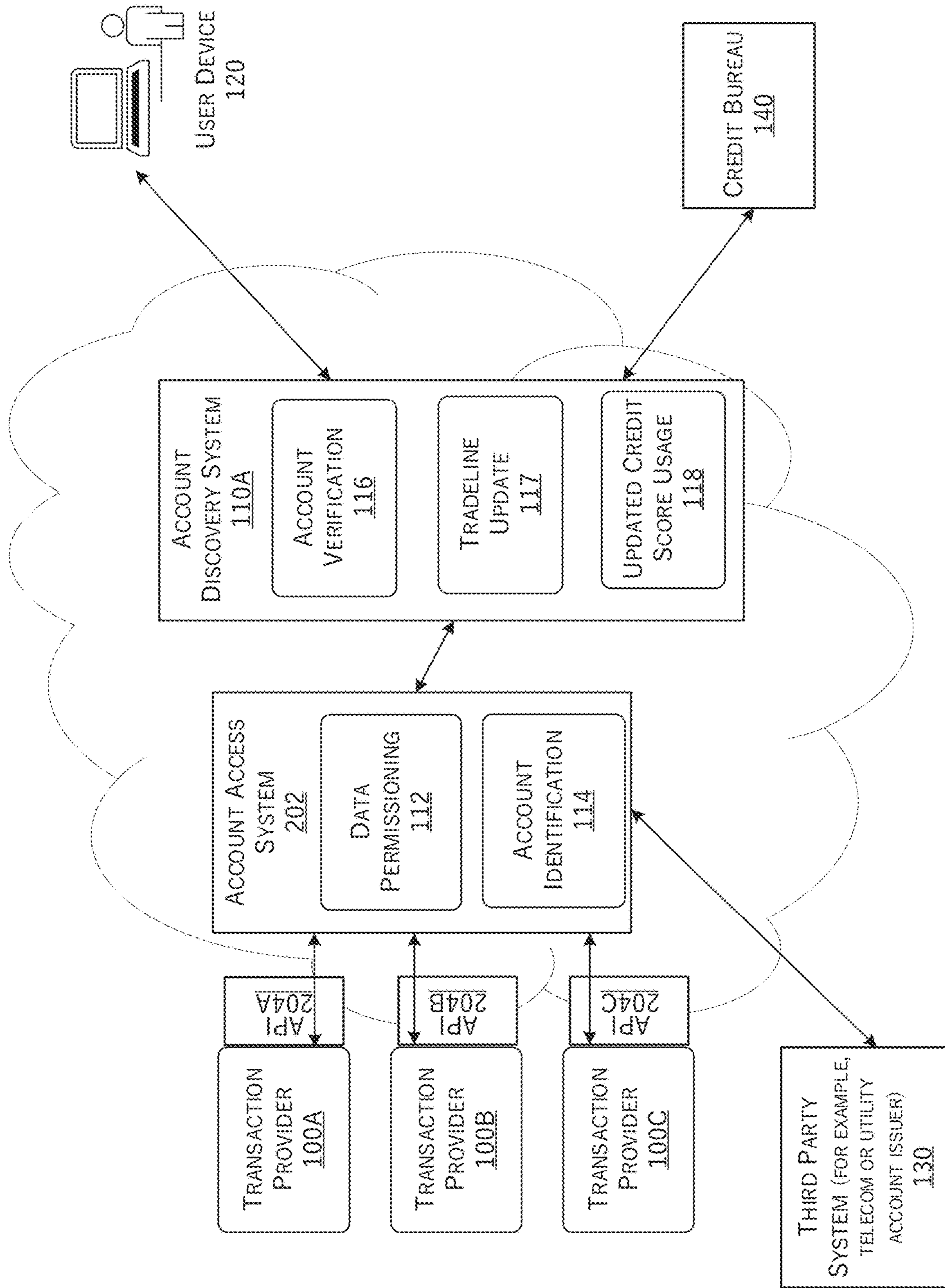


FIGURE 6

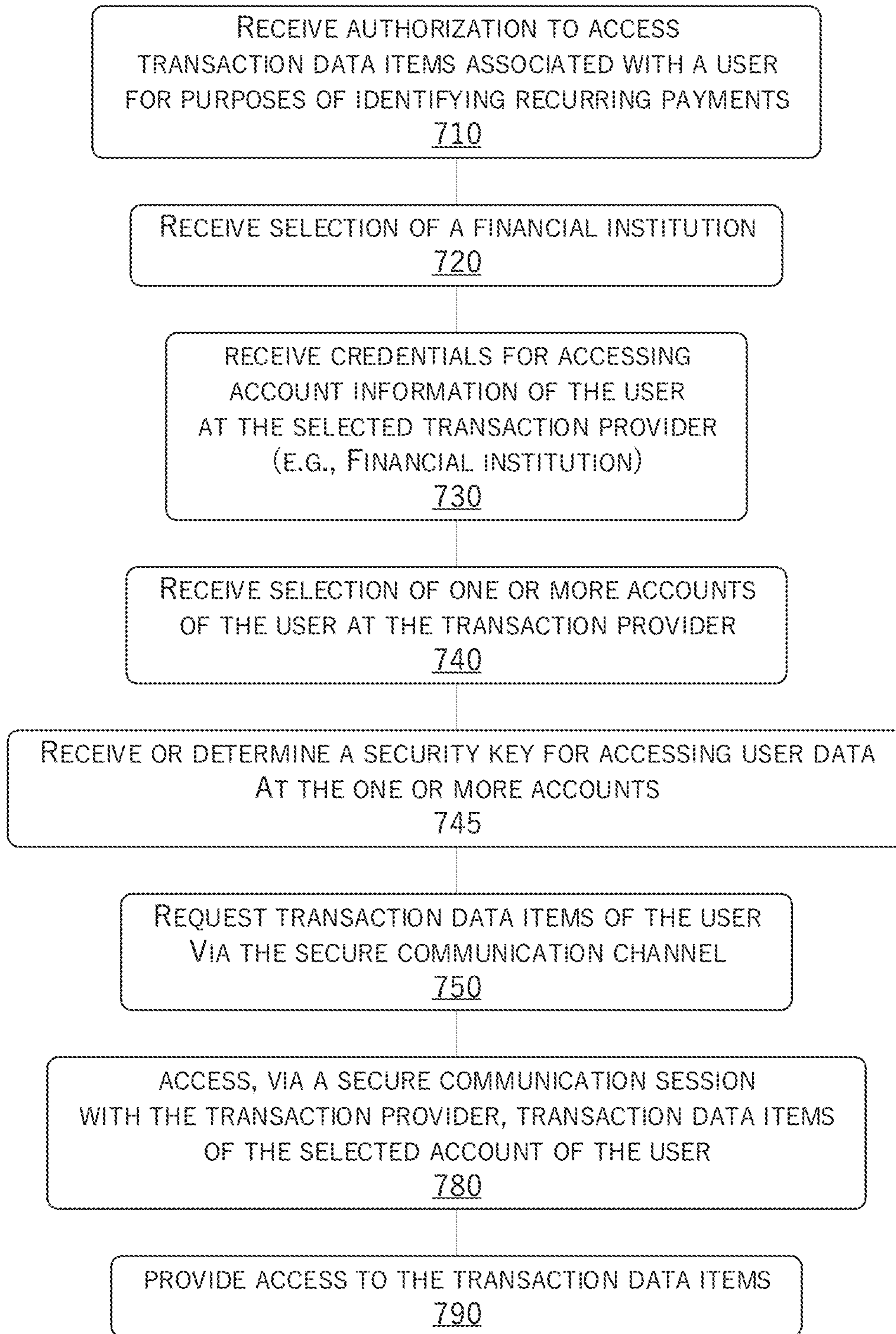


FIGURE 7

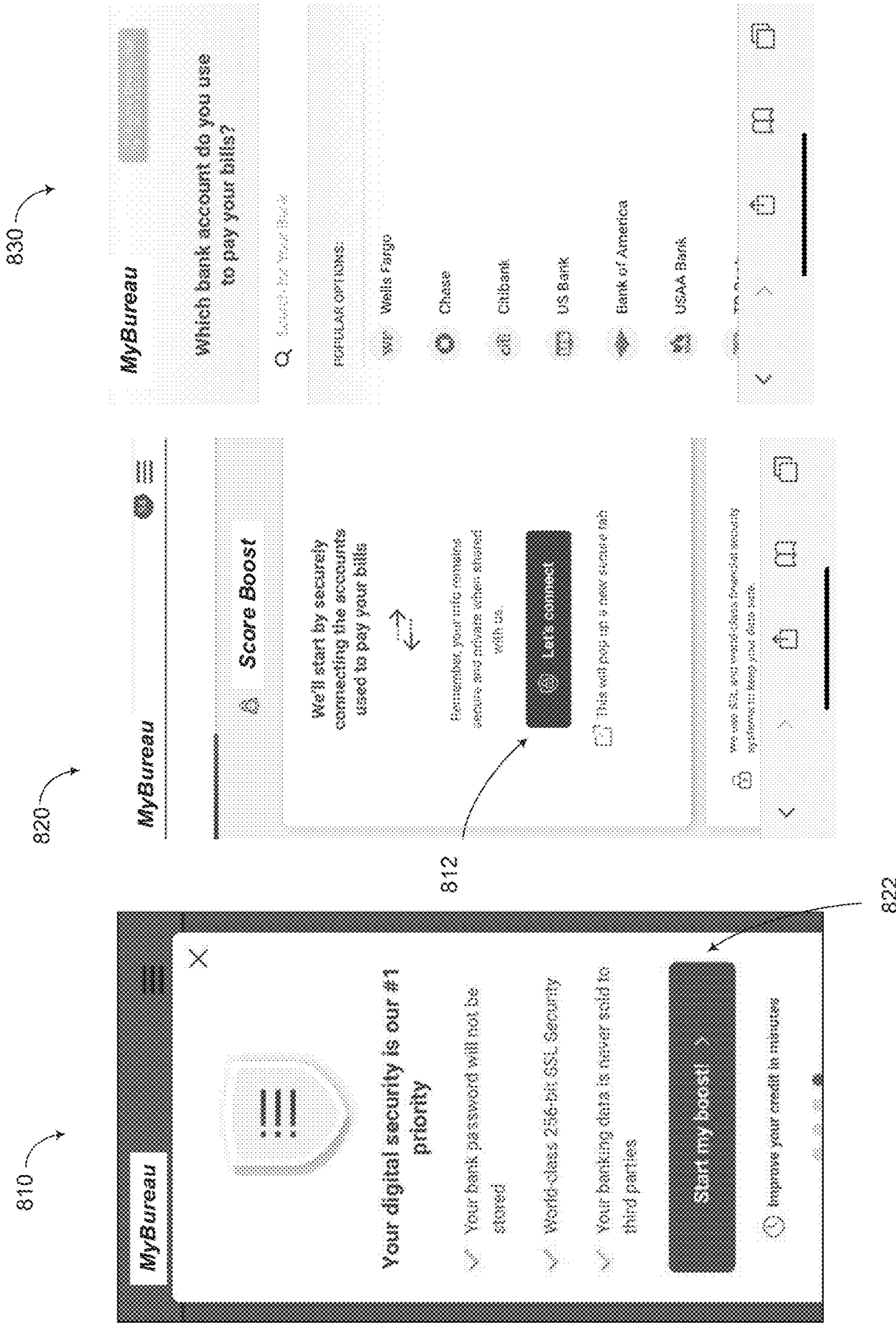


FIGURE 8

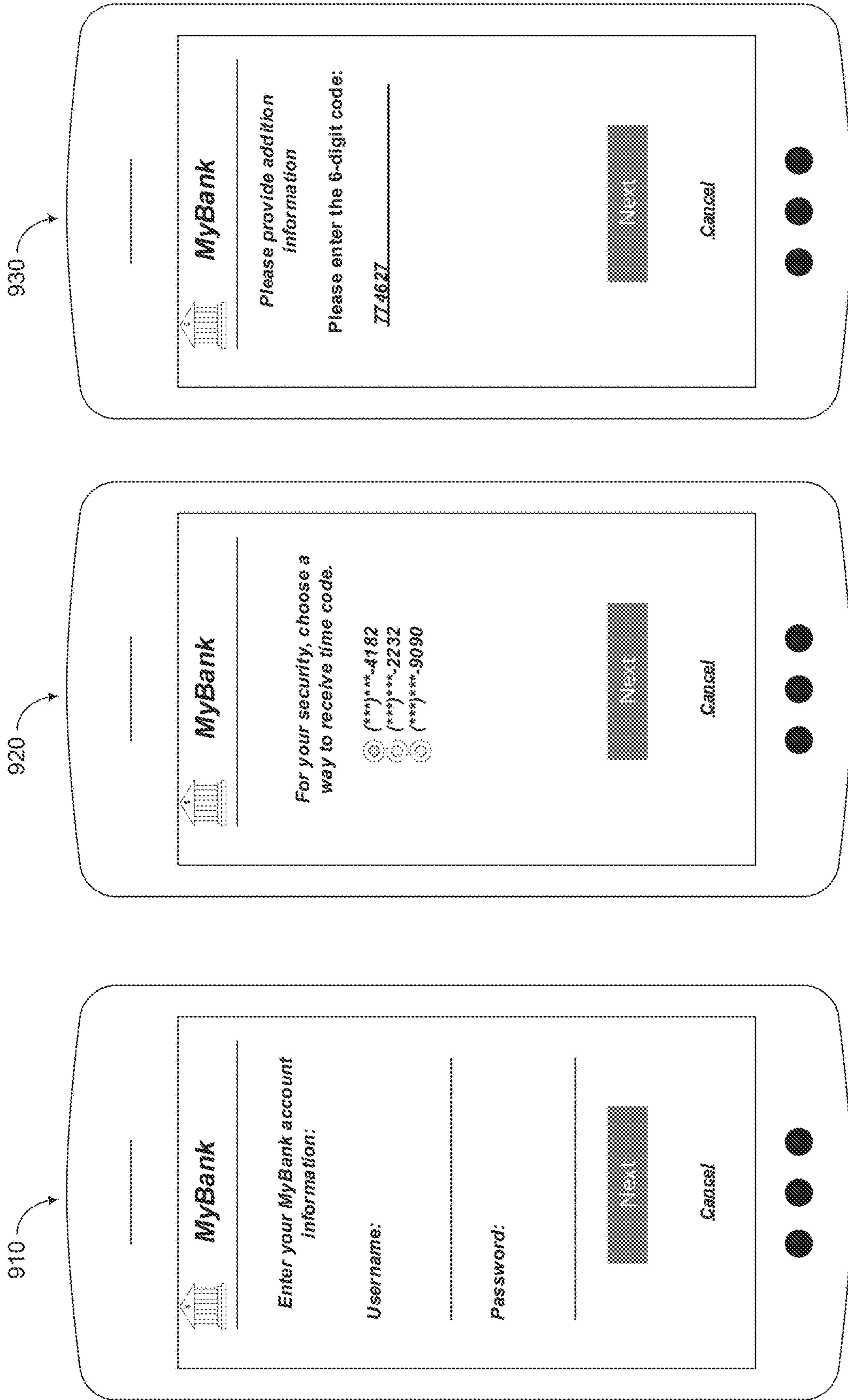


FIGURE 9

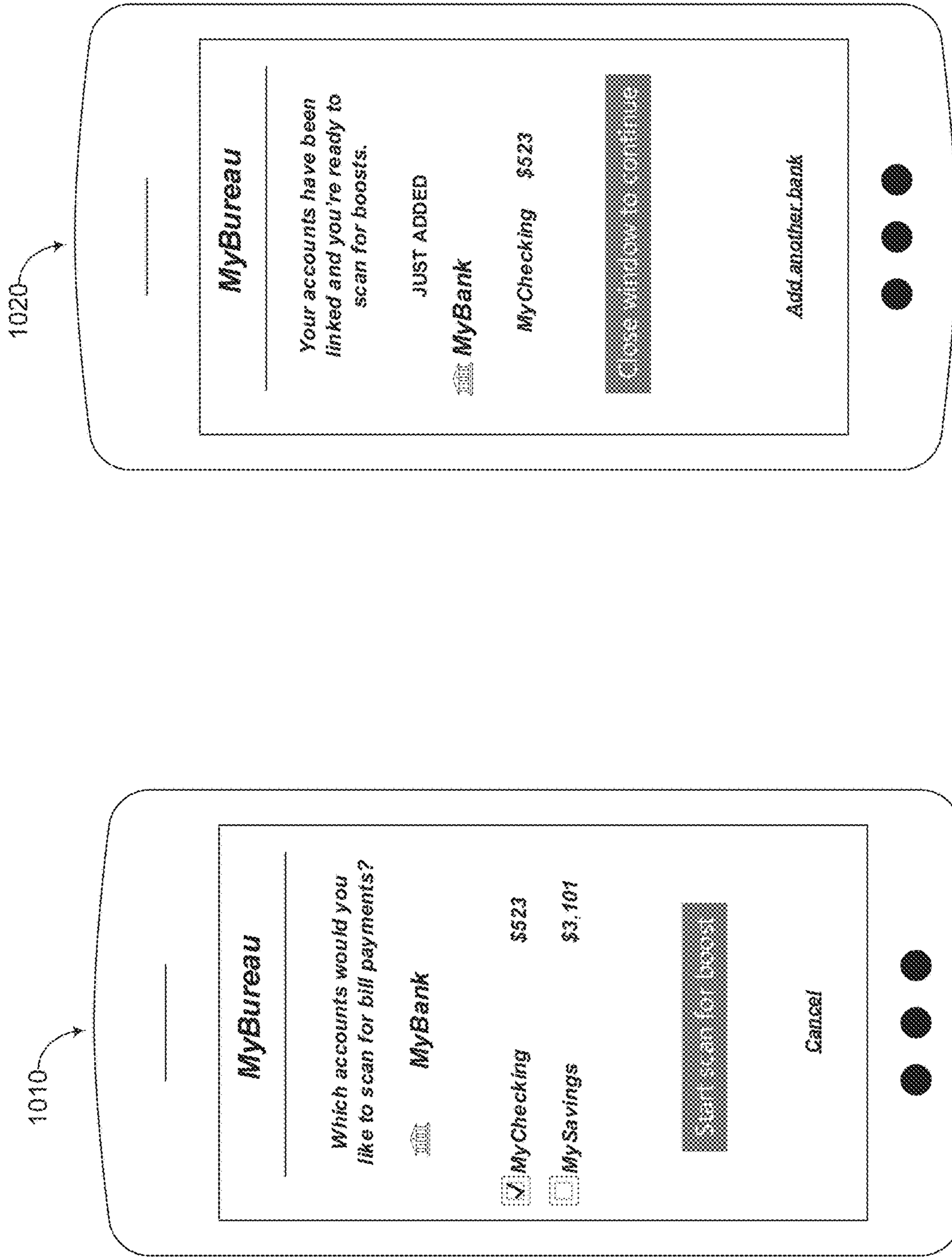


FIGURE 10

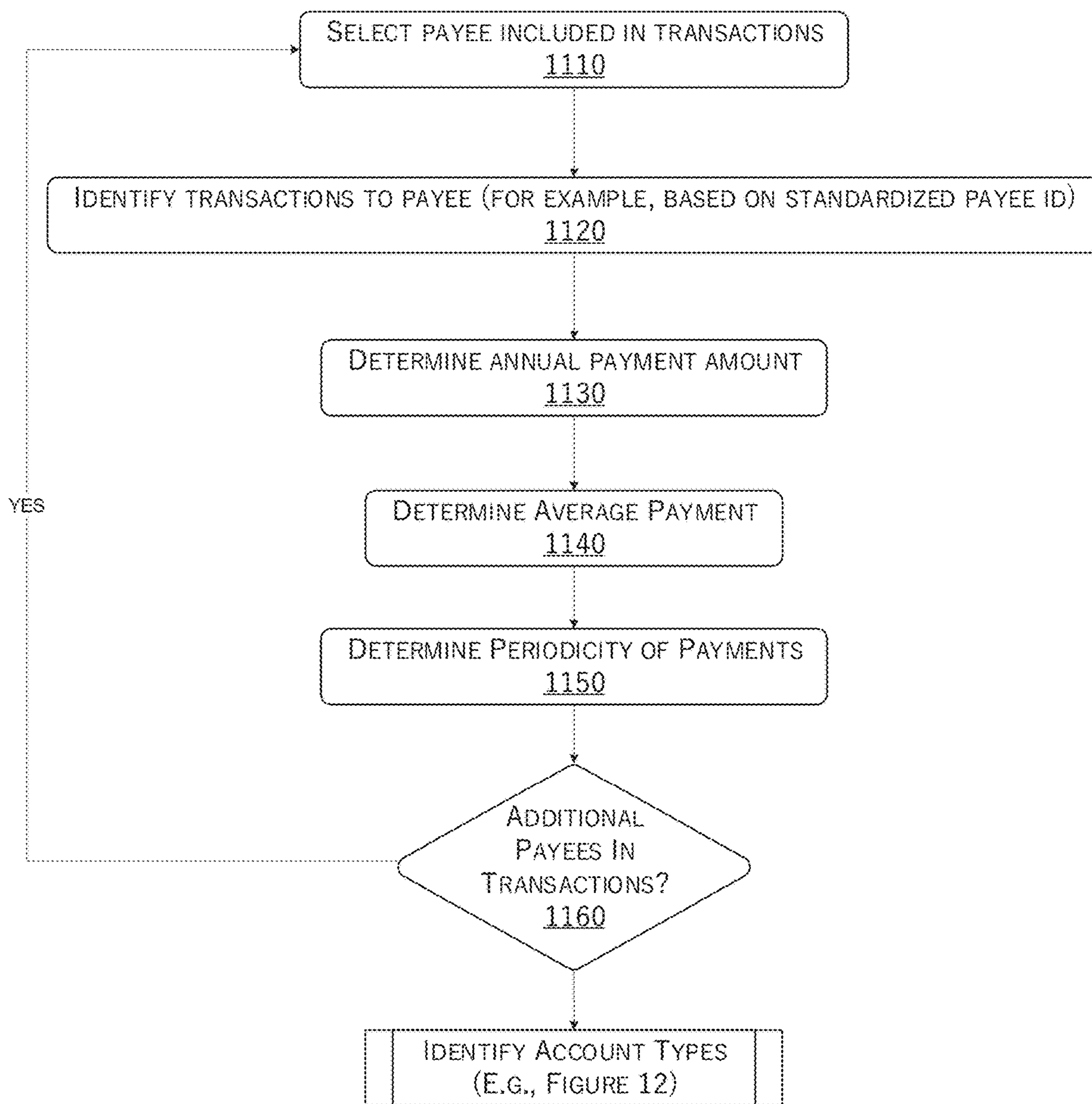


FIGURE 11

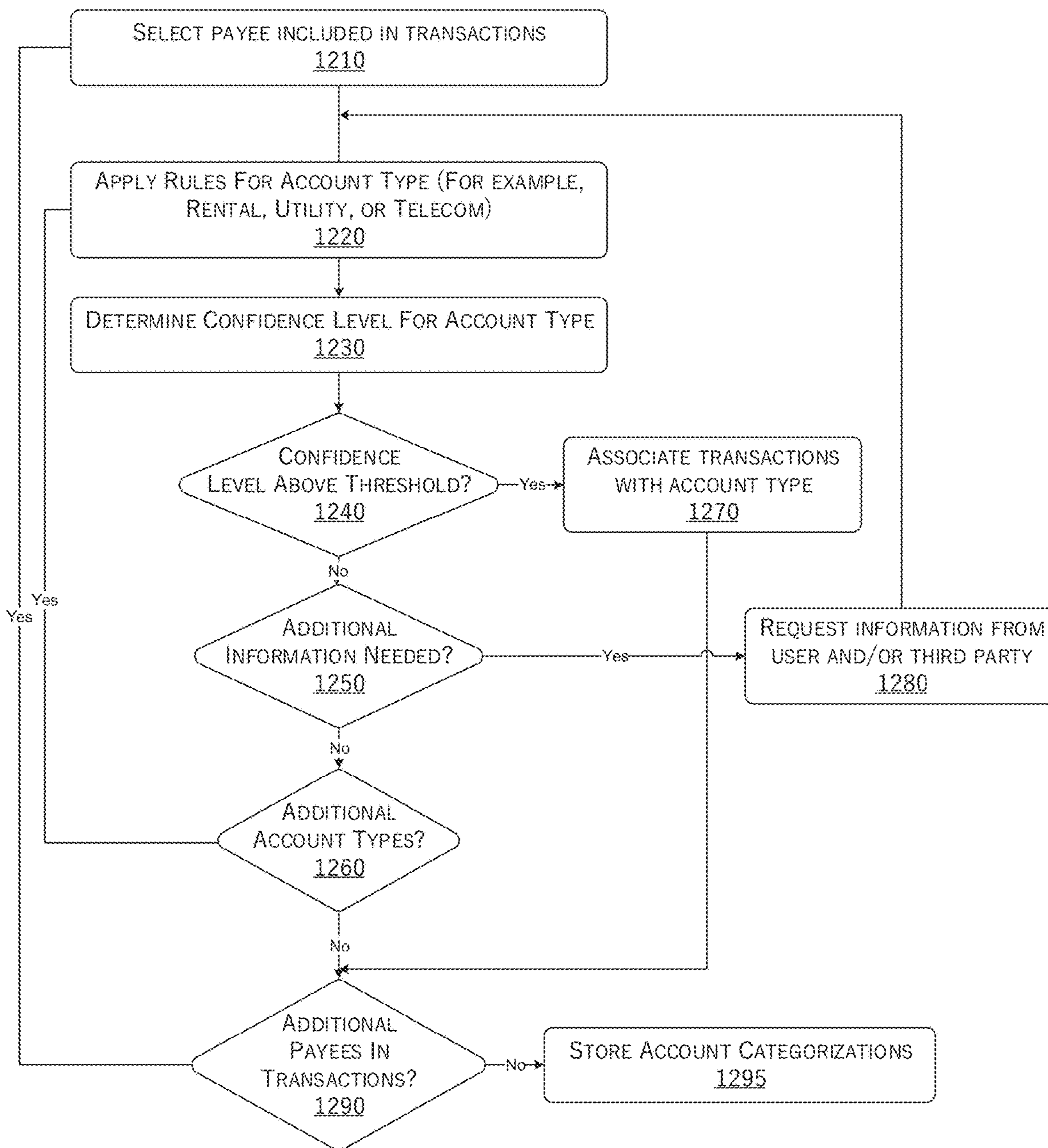


FIGURE 12

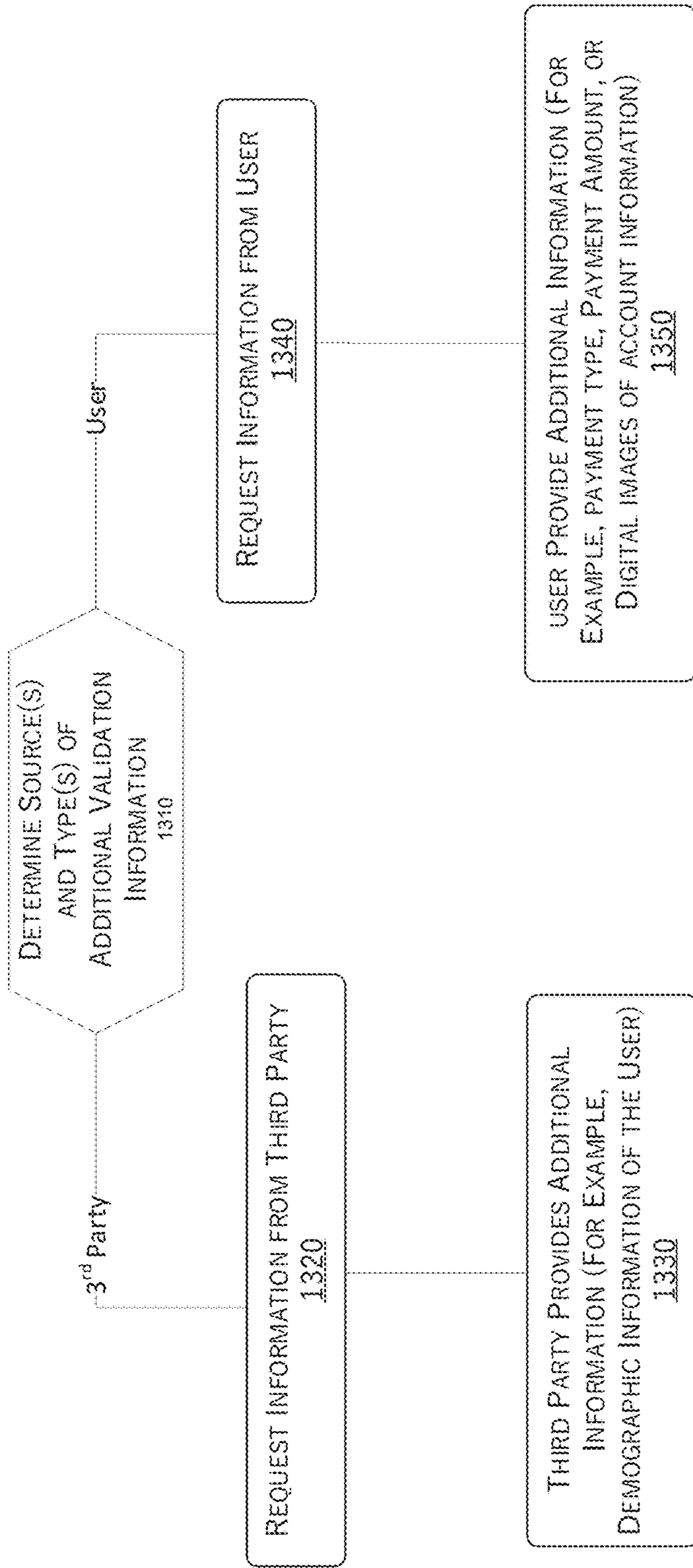


FIGURE 13

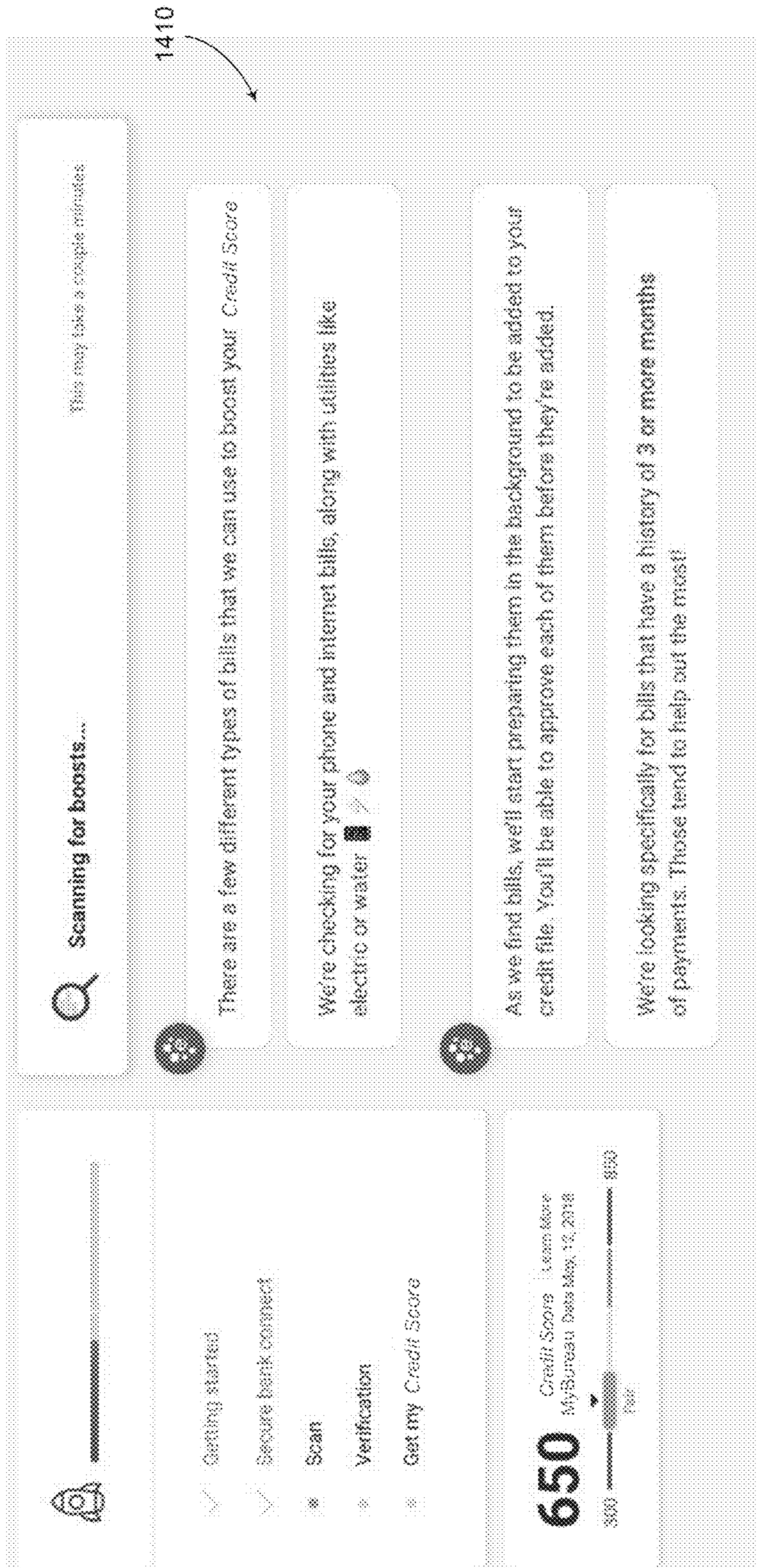


FIGURE 14

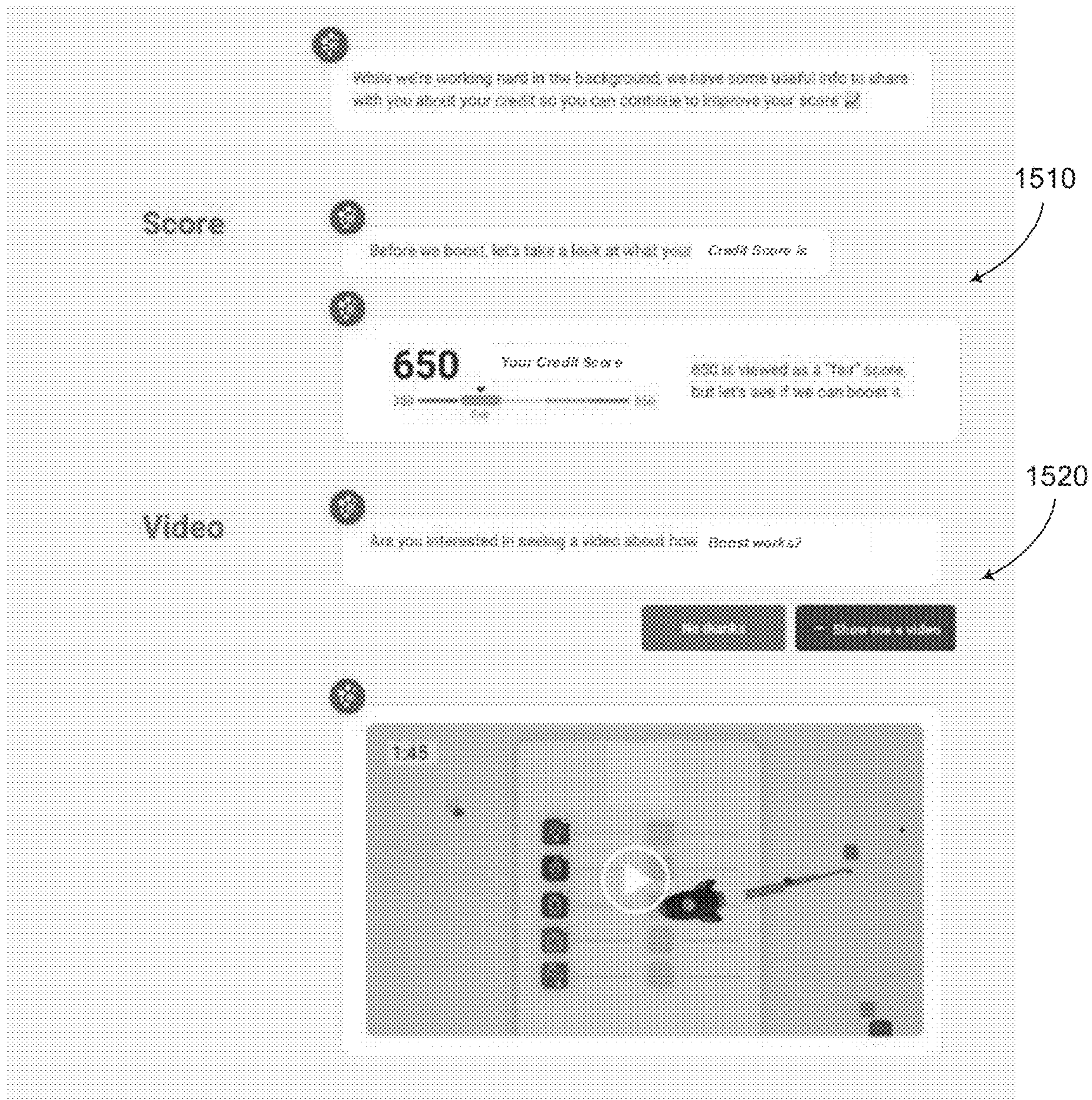


FIGURE 15

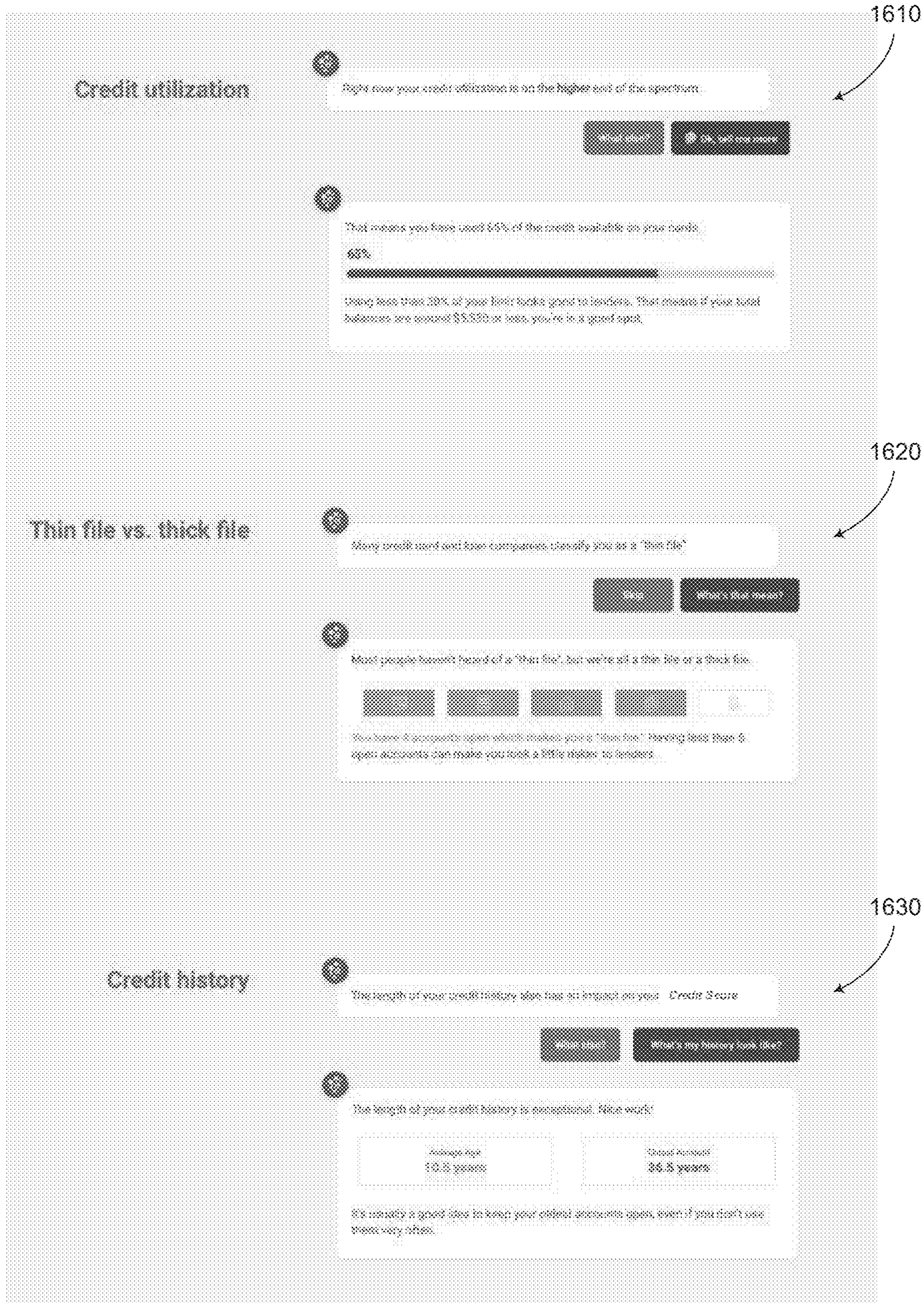


FIGURE 16

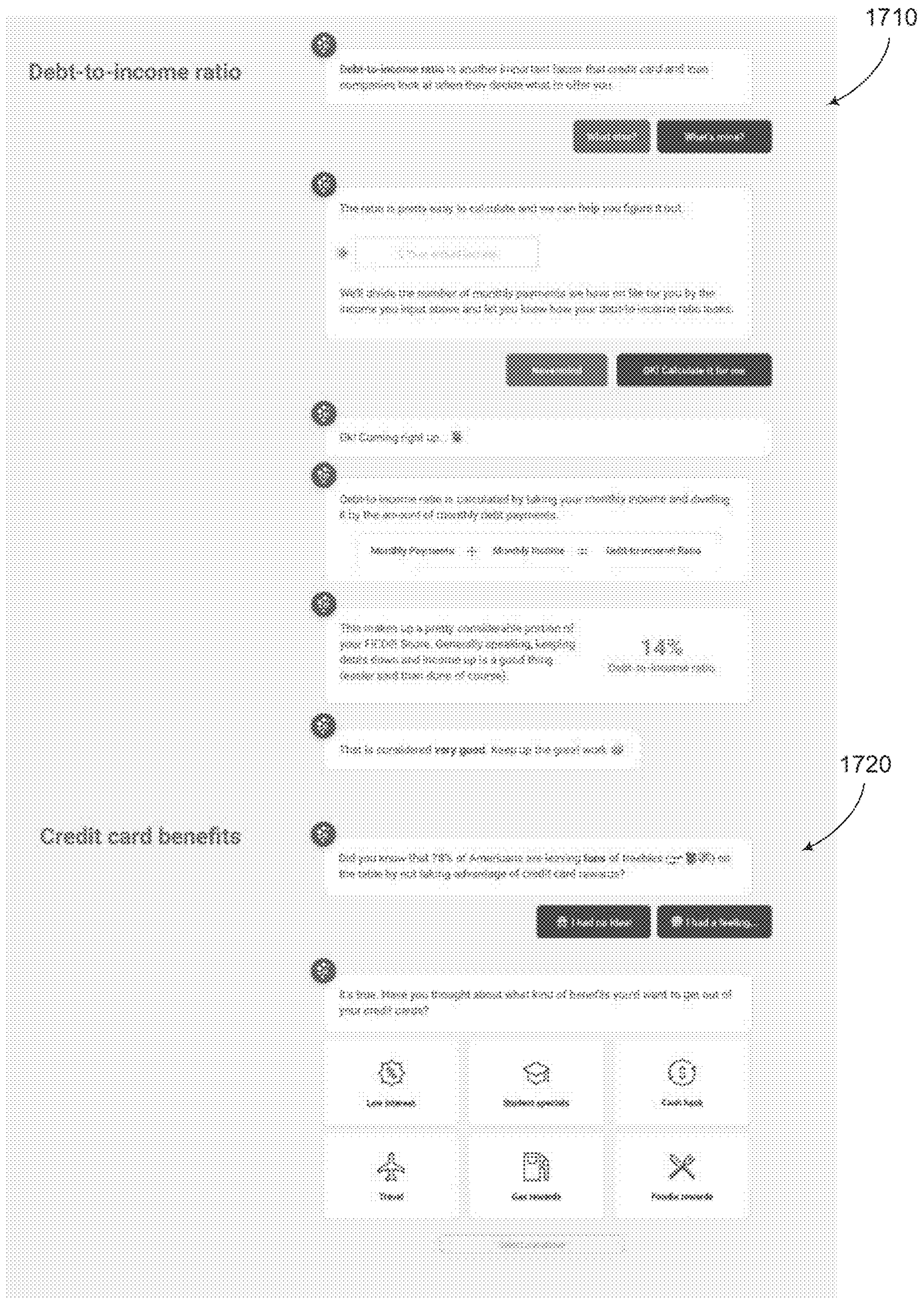


FIGURE 17

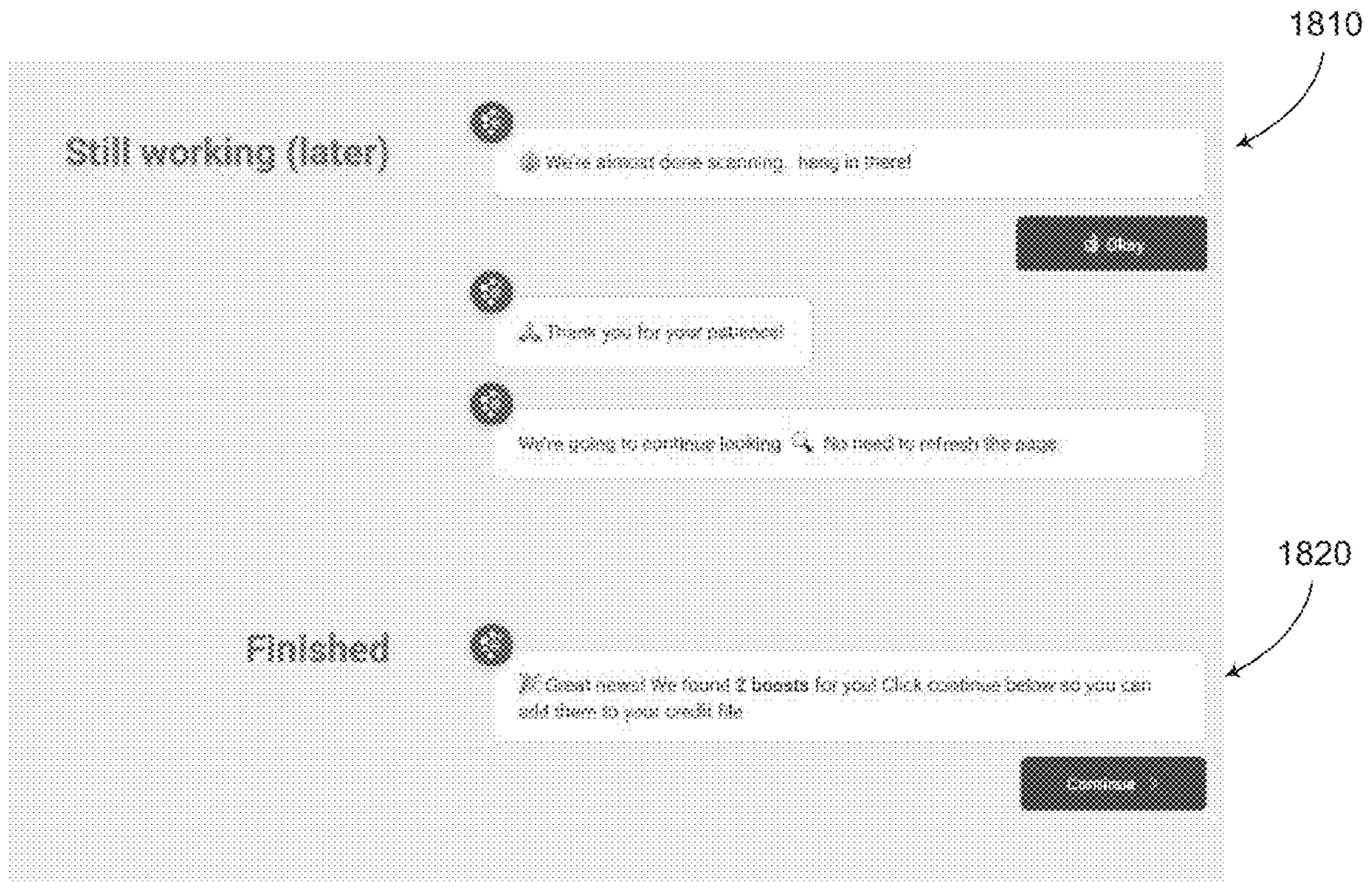


FIGURE 18

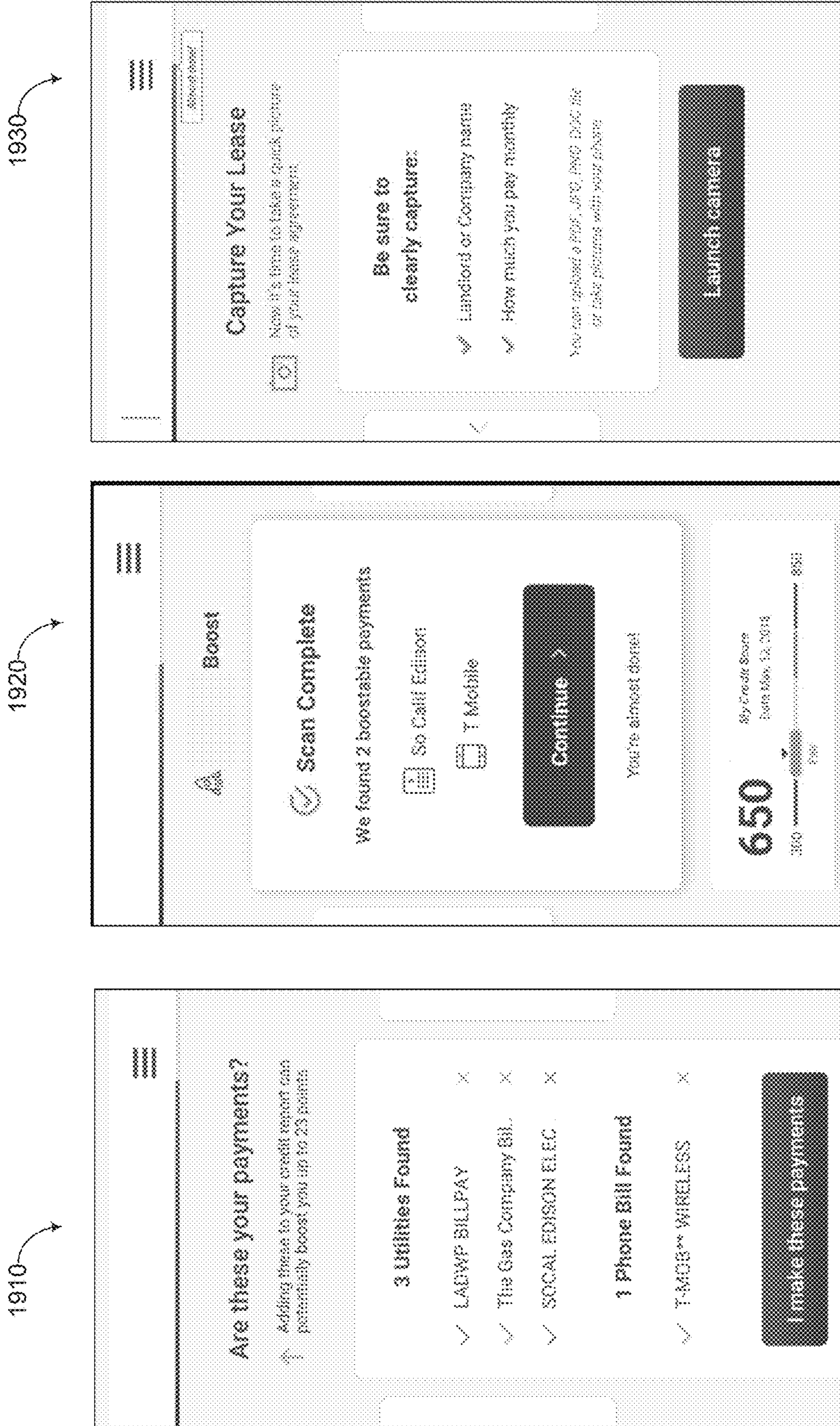


FIGURE 19

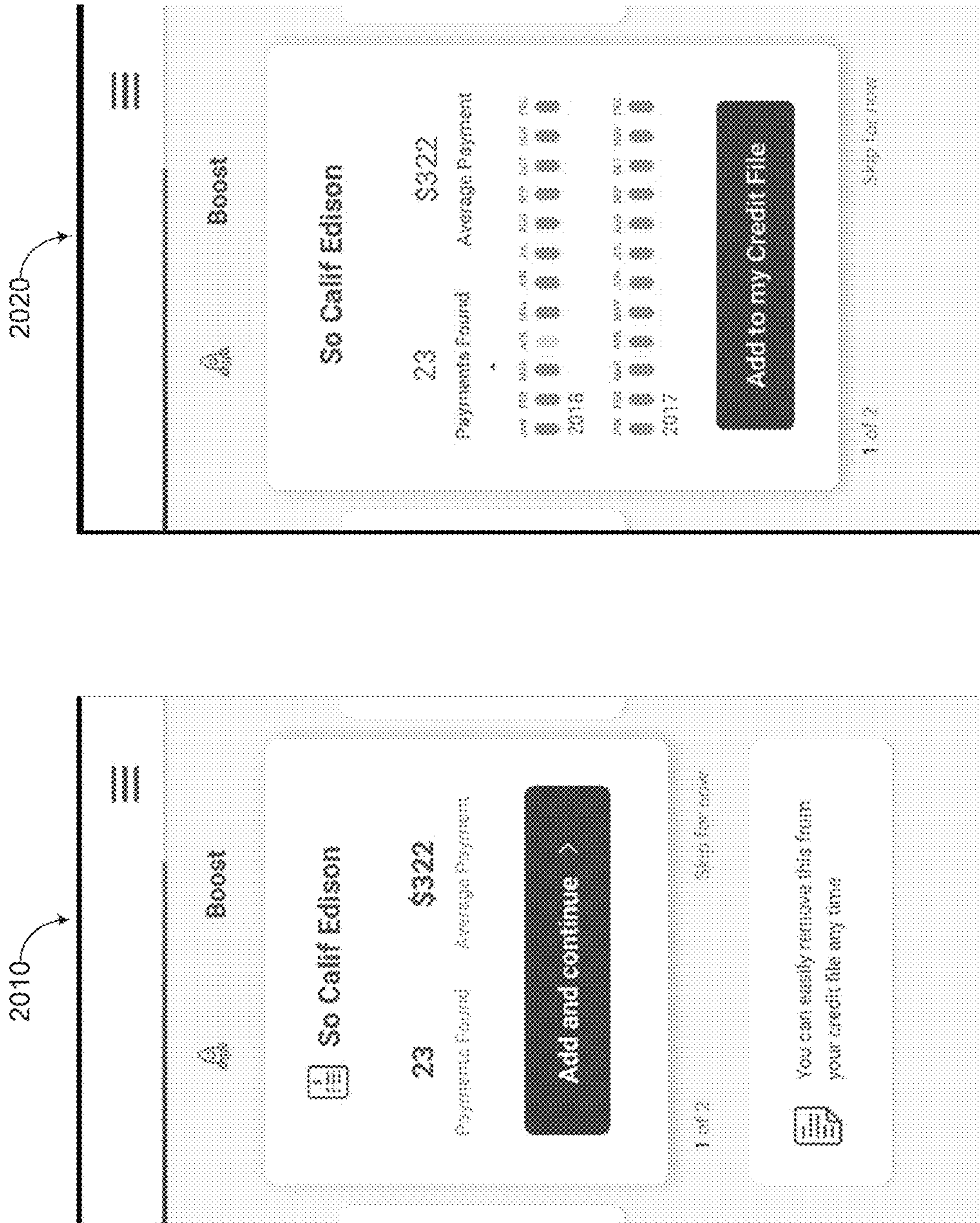
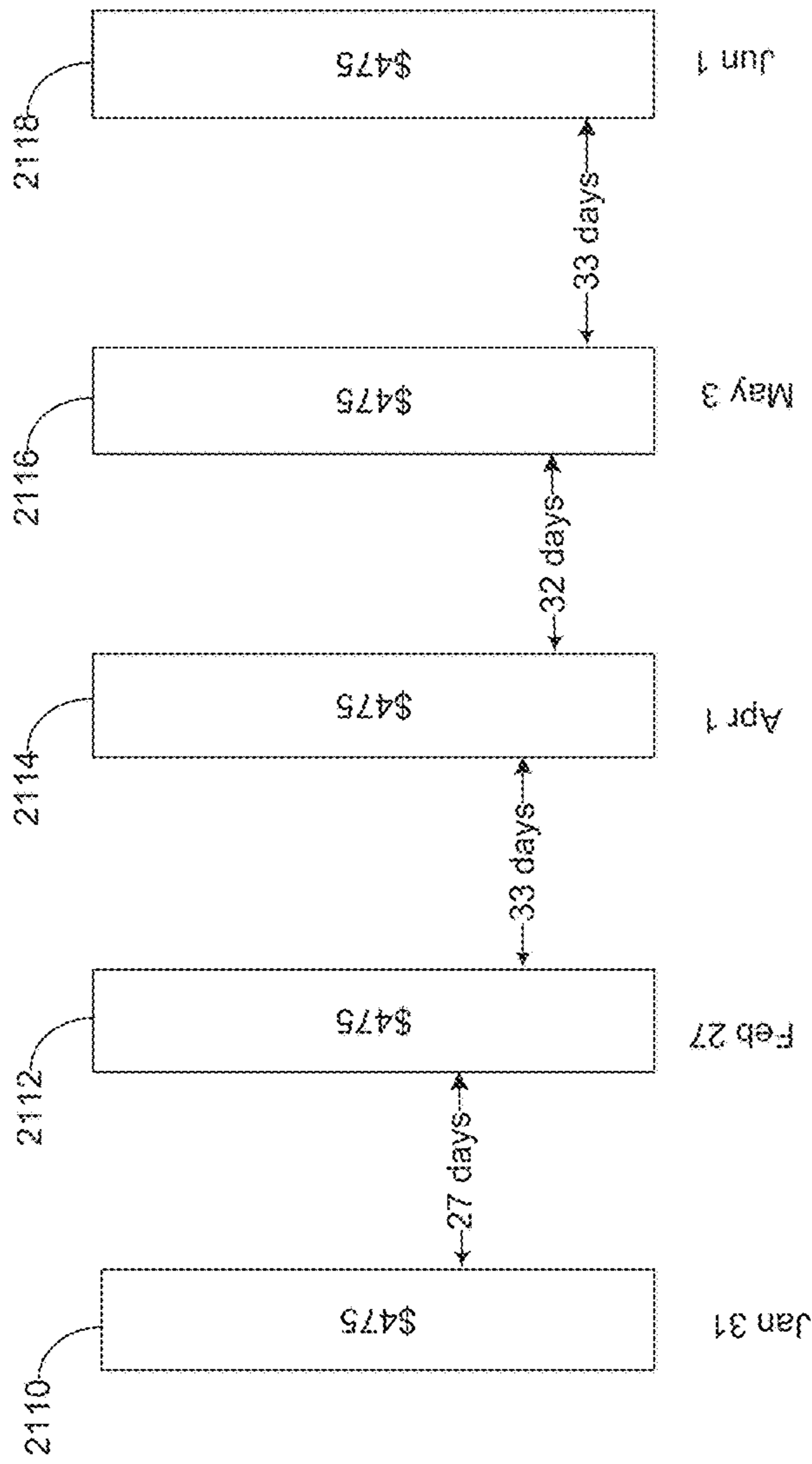
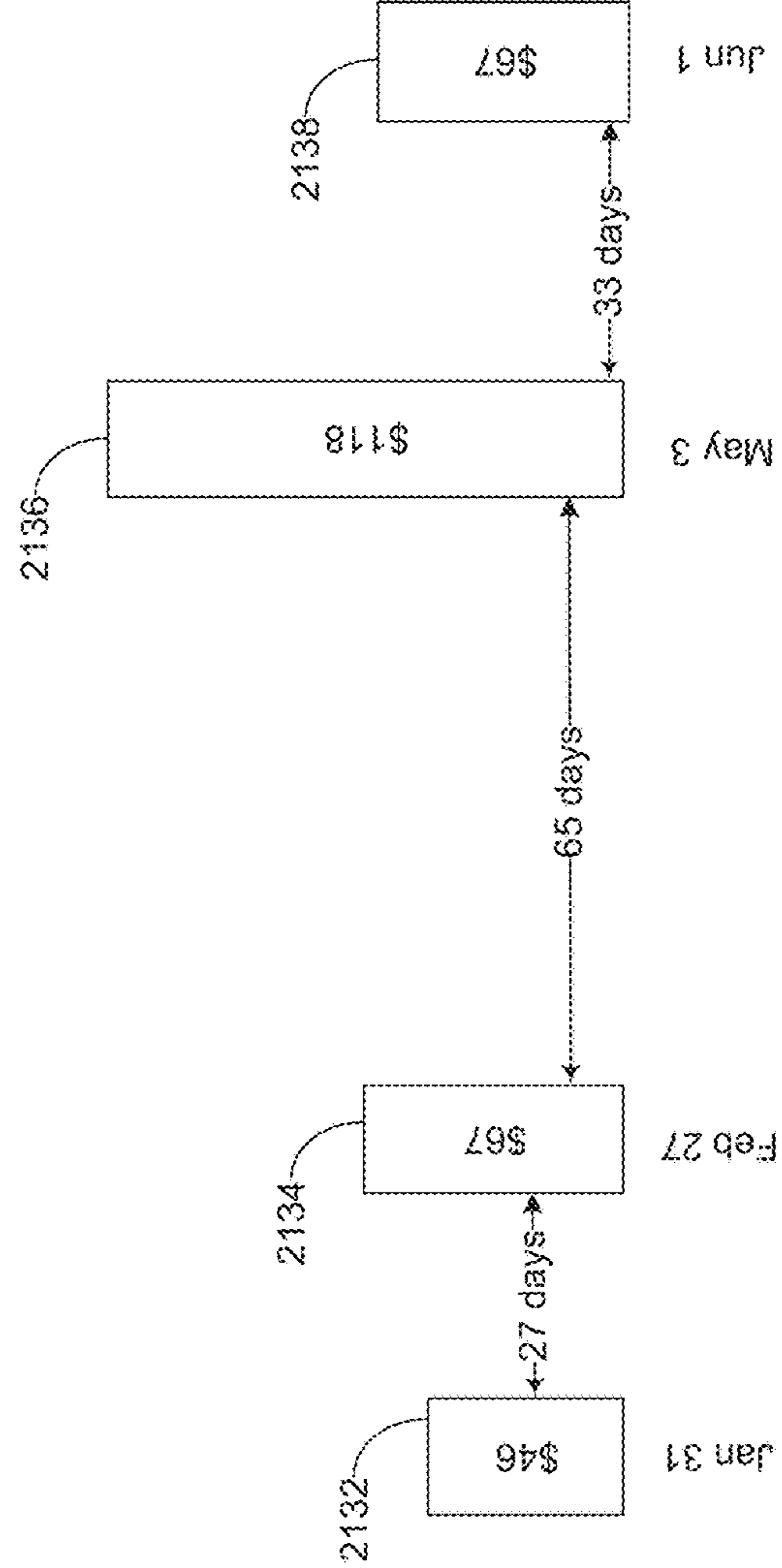


FIGURE 20



Payee: BIG LANDLORD
 Payments: 5
 Months: 5
 Average Payment: \$475
 Average Days Between
 Payments: 31.25

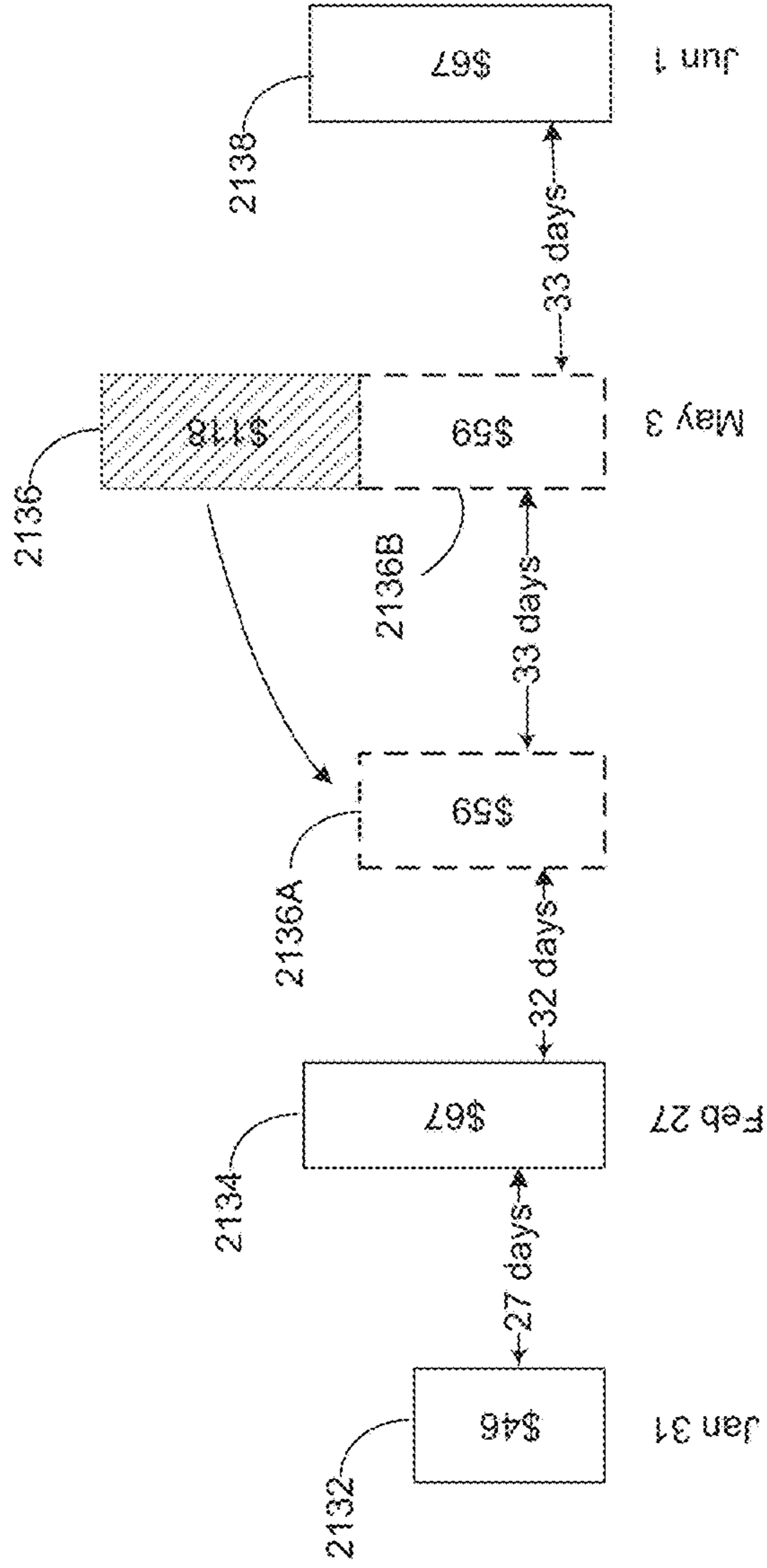
2120



Payee: ABC MOBILE
 Payments: 4
 Months: 5
 Average Payment: \$74.5
 Average Days Between
 Payments: 41.7

2130

FIGURE 21



Payee: ABC MOBILE
 Payments: 4
 Months: 5
 Average Payment: \$74.5
 Average Days Between
 Payments: 41.7

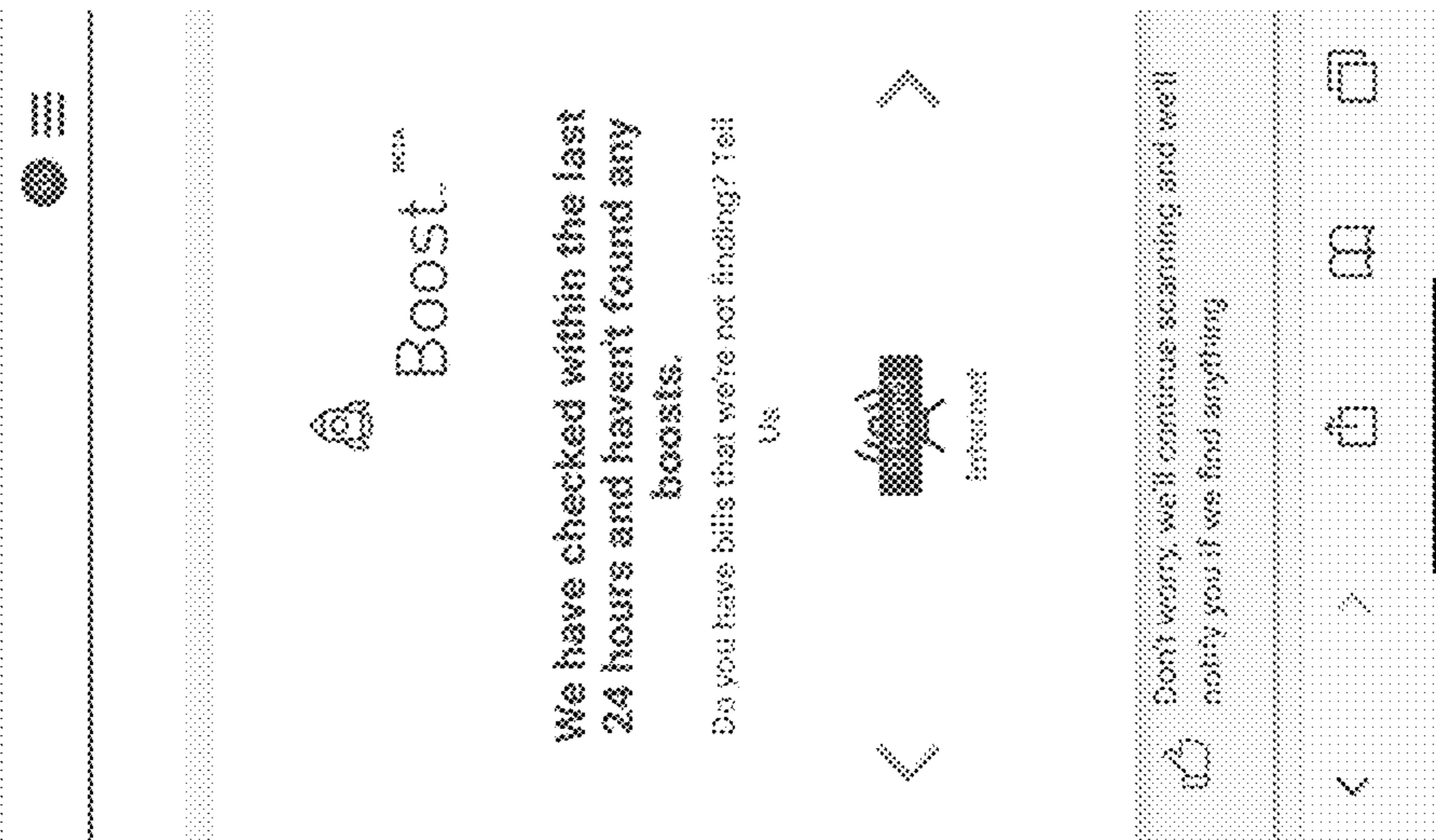
2130

Payee: ABC MOBILE
 Modeled Payments: 5
 Months: 5
 Modeled Average Payment: \$59.6
 Modeled Average Days Between
 Payments: 31.25

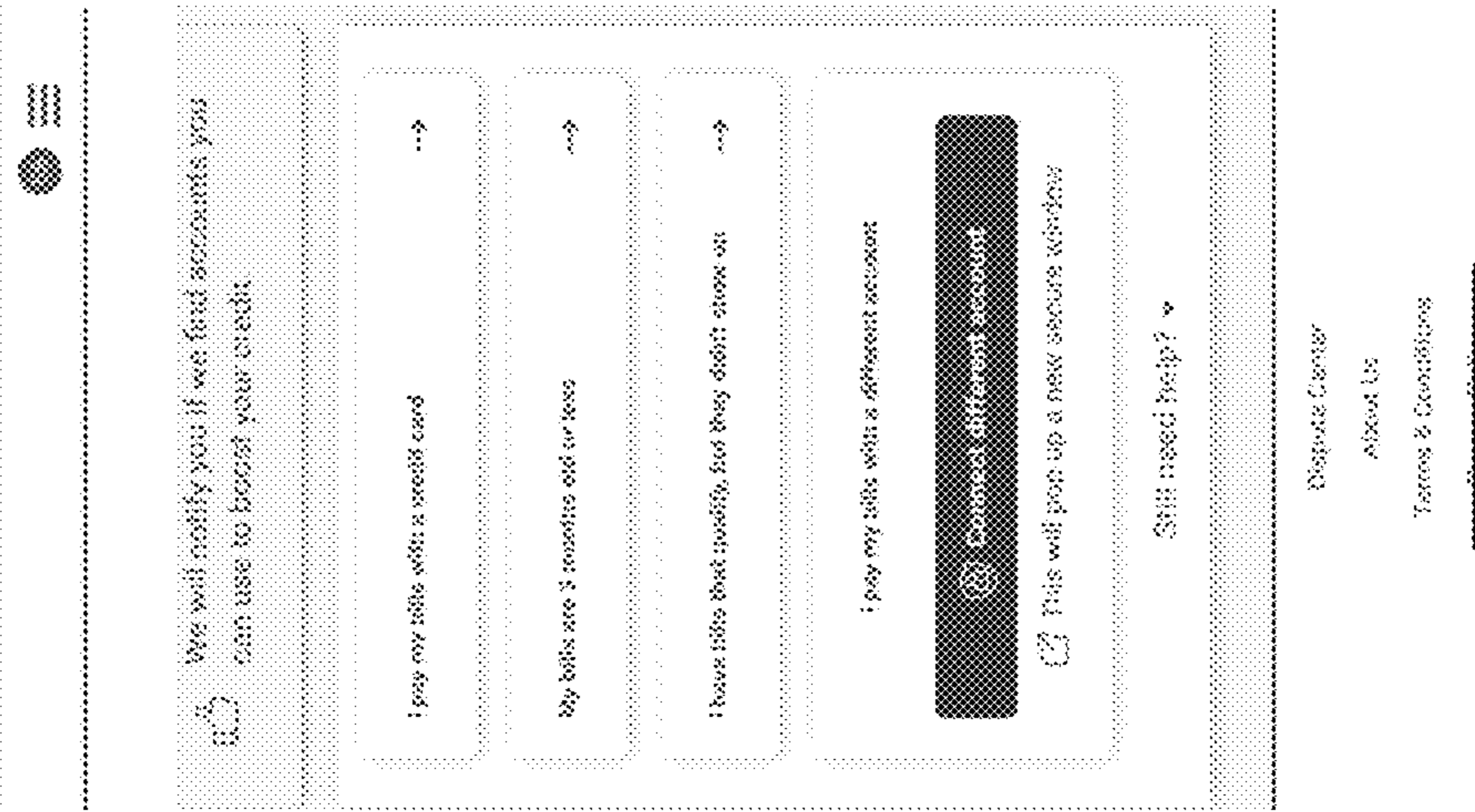
2210

FIGURE 22

2310



2320



2330

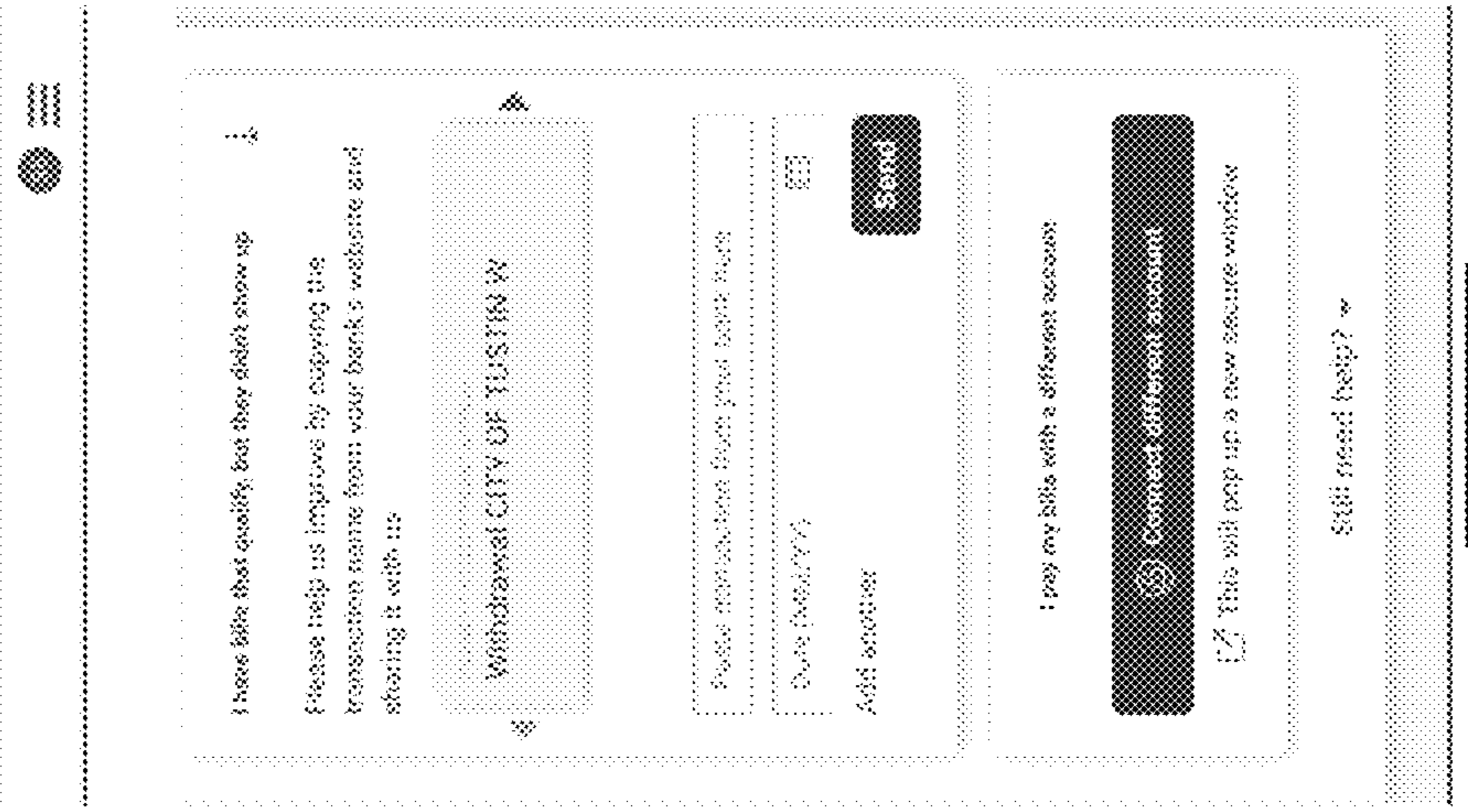


FIGURE 23

2410

Boost 1 of 2

SO CAL EDISON BILLPAY

Verify your payments before adding them to your Experian credit file.

21 Payments Found

Utility Boost Type

\$161 Average Payment

Payment History

Year	jan	feb	mar	apr	may	jun	jul	aug	sep	oct	nov	dec
2017	●	●	●	●	●	●	●	●	●	●	●	●
2018	●	●	●	●	●	●	●	●	●	●	●	●

● Payment found ● Data unavailable

Add to my Credit File

Skip for now

2412

FIGURE 24A

2420 ↘

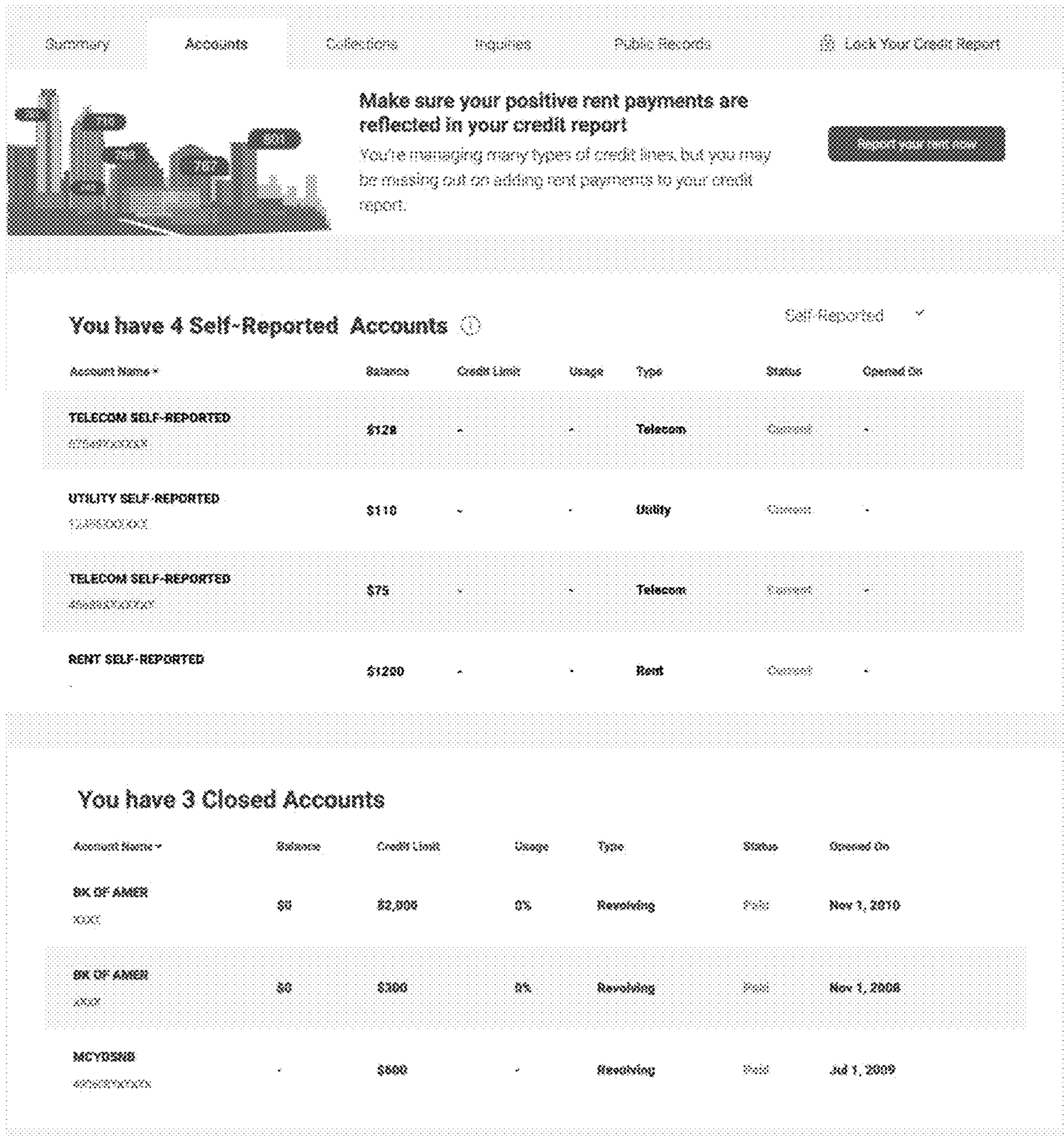


FIGURE 24B

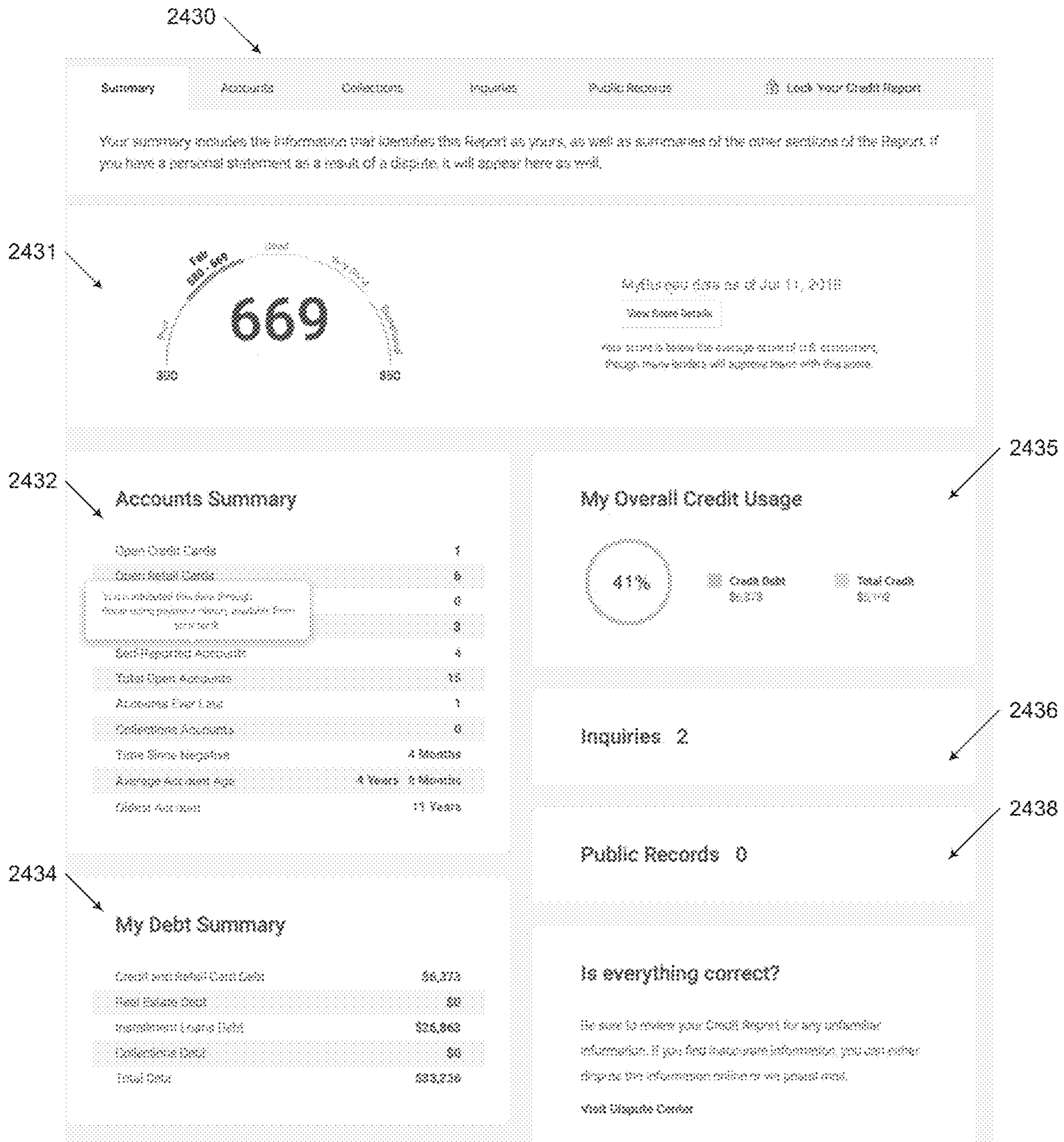


FIGURE 24C

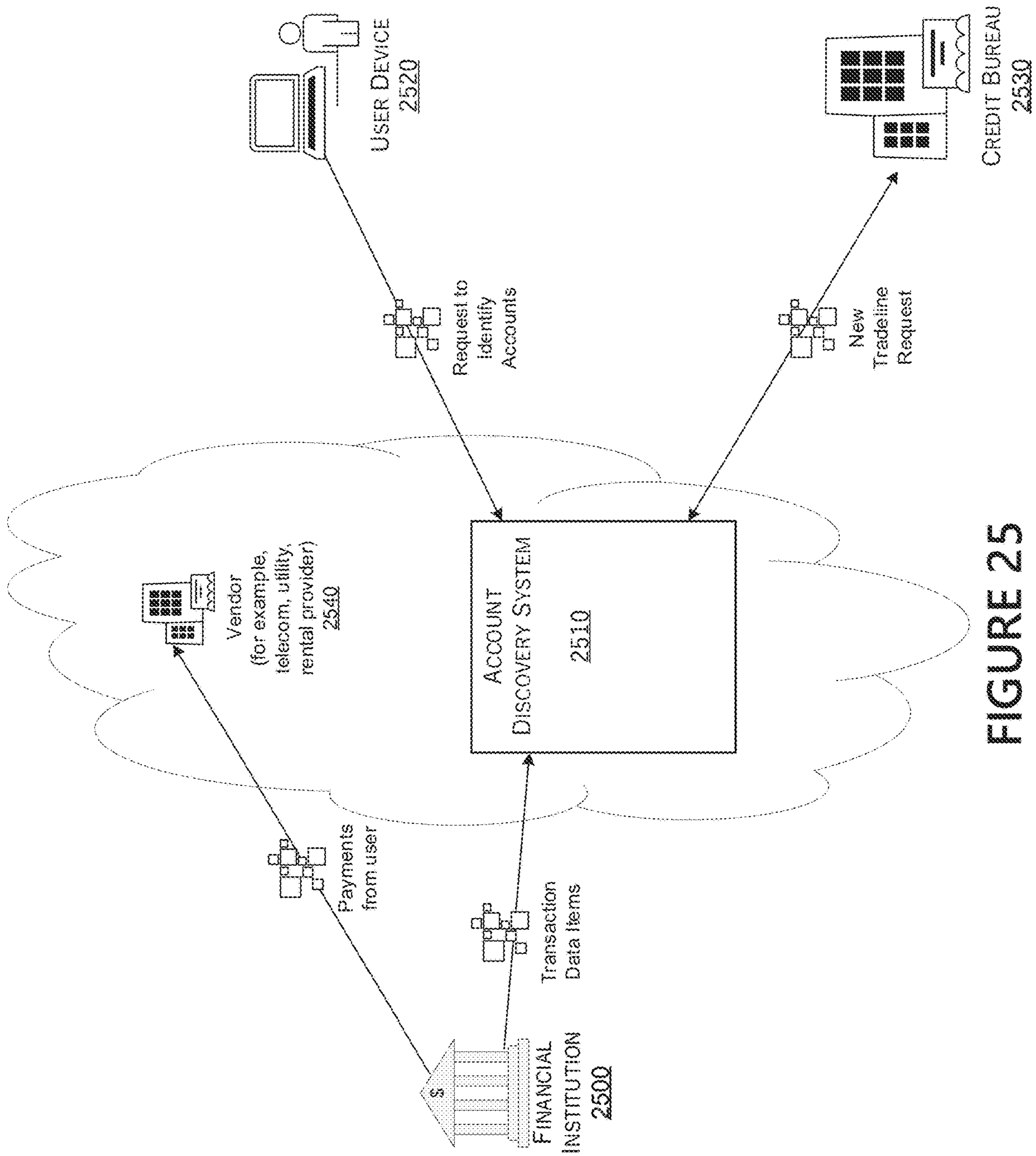


FIGURE 25

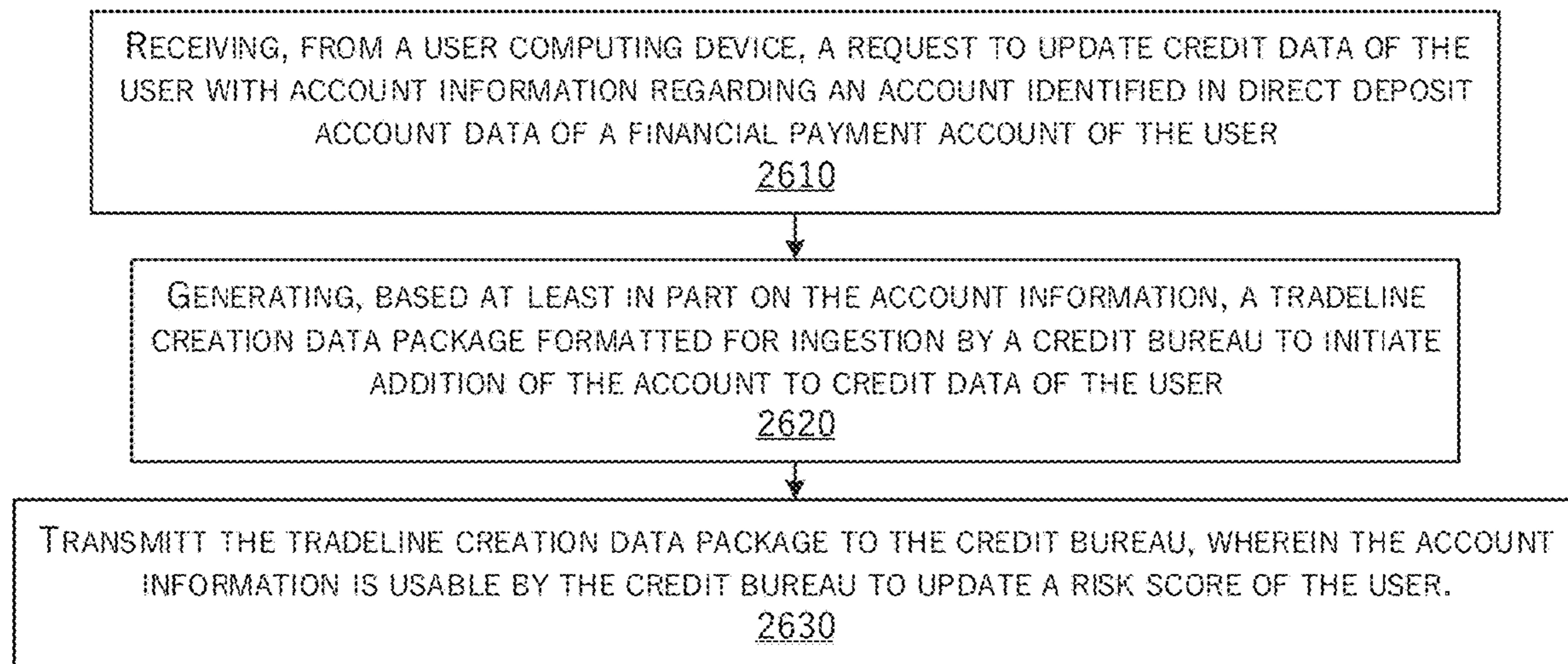


FIGURE 26

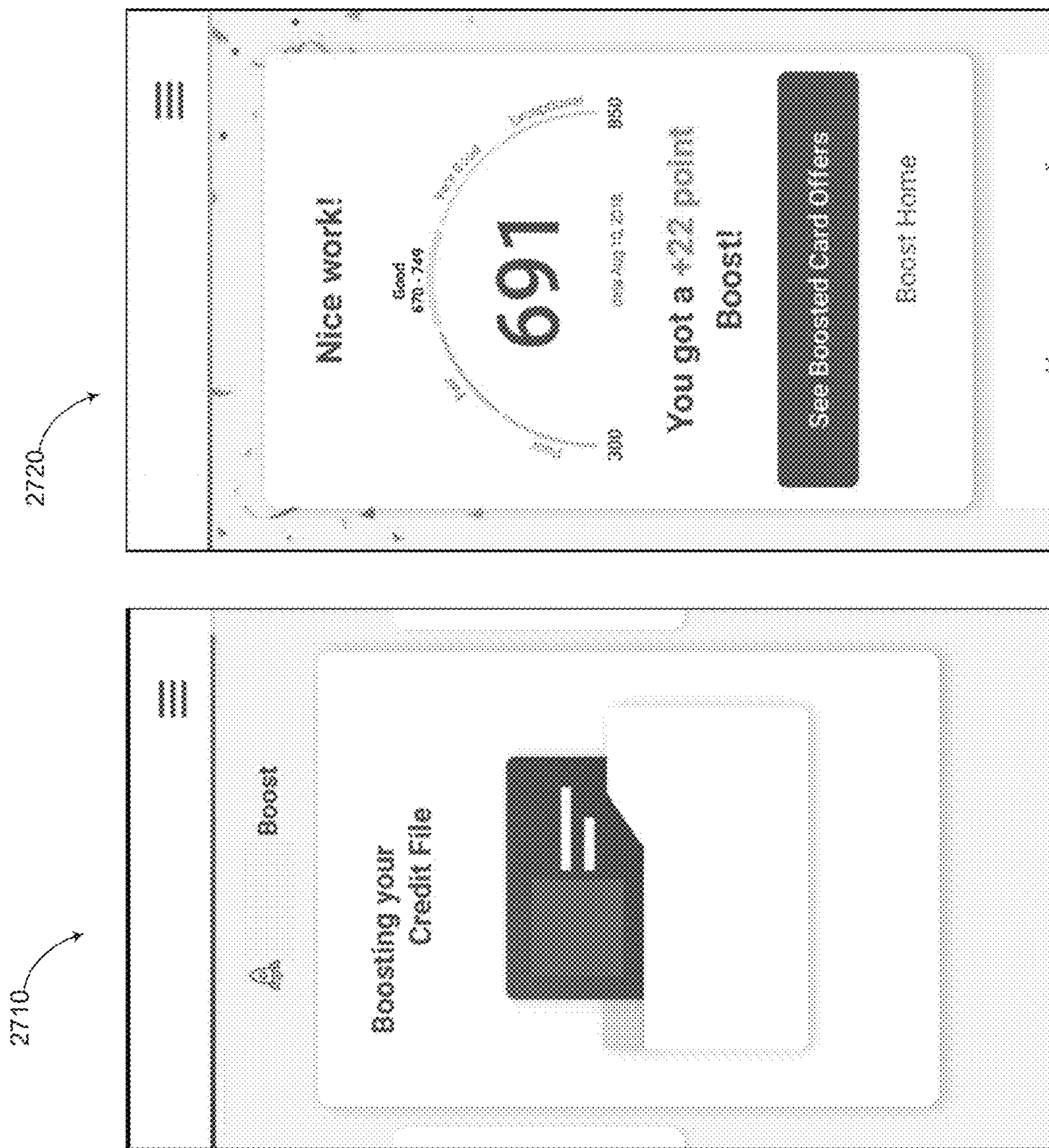


FIGURE 27

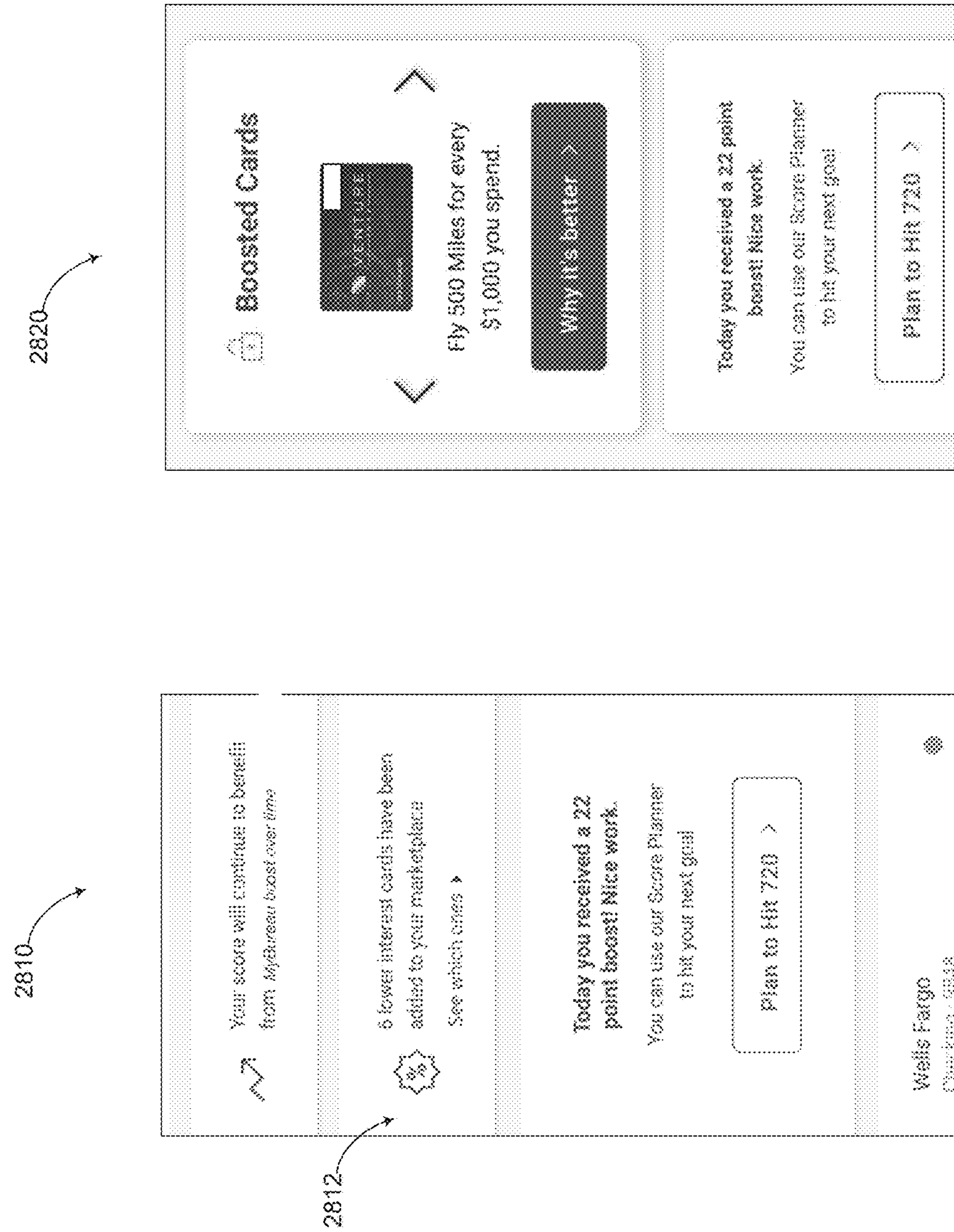


FIGURE 28A

2830

Great news! Your new score is opening doors to attractive new options.

Who noticed your new score
YourBank Credit Card

Why it's special
Get unlimited 1.5% cash back on every purchase, every day.

Who noticed your new score
YourBank Credit Card

Why it's special
You fly 1.8 miles for every dollar you spend on this card.

We had 4 other credit cards that liked your new score. Want to see them?

Expensin Partner Offer

I've boosted, now what?
A higher credit score can give you the ability to get approved for credit cards and loans. Keep paying your bills on time and improving your credit score, and you will get access to the best terms for credit cards and loans -- even credit card rewards like cash back or travel perks.

Advertiser Disclosure

2832

2834

FIGURE 28B

2840

Your Next Credit Report is available in 28 days.

Summary Accounts Collections Inquiries Public Records Lock Your Credit Report

Utility Self-Reported [View All Accounts + Previous](#) [Next](#)

You added this account to your history earlier than expected. You can remove it at any time.

Details

Account Number	44905XXXXXX
Original Creditor	CHASE/SDGE Bill Pay
Company Sold	-
Account Type	Utility
Date Opened	-
Account Status	Open
Payment Status	Paid satisfactorily
Status Updated	June 30, 2018
Usage	-
Balance	\$128
Balance Updated	June 30, 2018
Original Balance	-
Monthly Payment	\$128
Payment Amount	-
Highest Balance	-
Terms	-
Responsibility	Indicated
Your Statement	-
Comments	-

MyBureau contact information
103 Main St
Anytown, AA 98765

Payment History

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2017	On time	On time	On time	On time	On time	On time	On time	On time	On time	On time	On time	On time
2018	On time	On time	On time	On time	On time	On time	On time	On time	On time	On time	On time	On time

2842 [Remove this account](#)

FIGURE 28C

2850

Filter by

All

Revolving Accounts

Installment Loans

Real Estate Loans

Self-Reported Accounts

sort by

Alphabetical

Date Opened

Status

Self-Reported Accounts

Self-reported accounts are added through *add-new.html* and can be removed anytime. These accounts utilize available payment history (limited up to 24 months) from your bank, which you give us read-only access to. If you see any accounts or pending payments, it's possible that we have not yet received the most recent updates because *add-new.html* reports data to your credit file once a month. The account number listed on your *add-new.html* credit file is a tracking number generated by *add-new.html* and the account number of your bank or payer. Original creditor is the source of your self-reported data (your bank) and the payer (the company to which you pay your bills).

UTILITY SELF-REPORTED

XXXXXXXXXX

Status	Open/Never late
Account Type	Utility
Recent Payment Amount	\$100
Original Creditor	DEK/SDOF Bill Pay
View	

RENT SELF-REPORTED

XXXXXXXXXX

Status	Open/Never late
Account Type	Rent
Recent Payment Amount	\$1200
Original Creditor	ChickGibson's Apts
View	

TELECOM SELF-REPORTED

XXXXXXXXXX

Status	Open/Never late
Account Type	Wireless
Recent Payment Amount	\$125
Original Creditor	ChickGibson Bill Pay
View	

UTILITY SELF-REPORTED

XXXXXXXXXX

Status	Open/Never late
Account Type	Utility
Recent Payment Amount	\$45
Original Creditor	ChickGibson Water Bill Pay
View	

FIGURE 28D

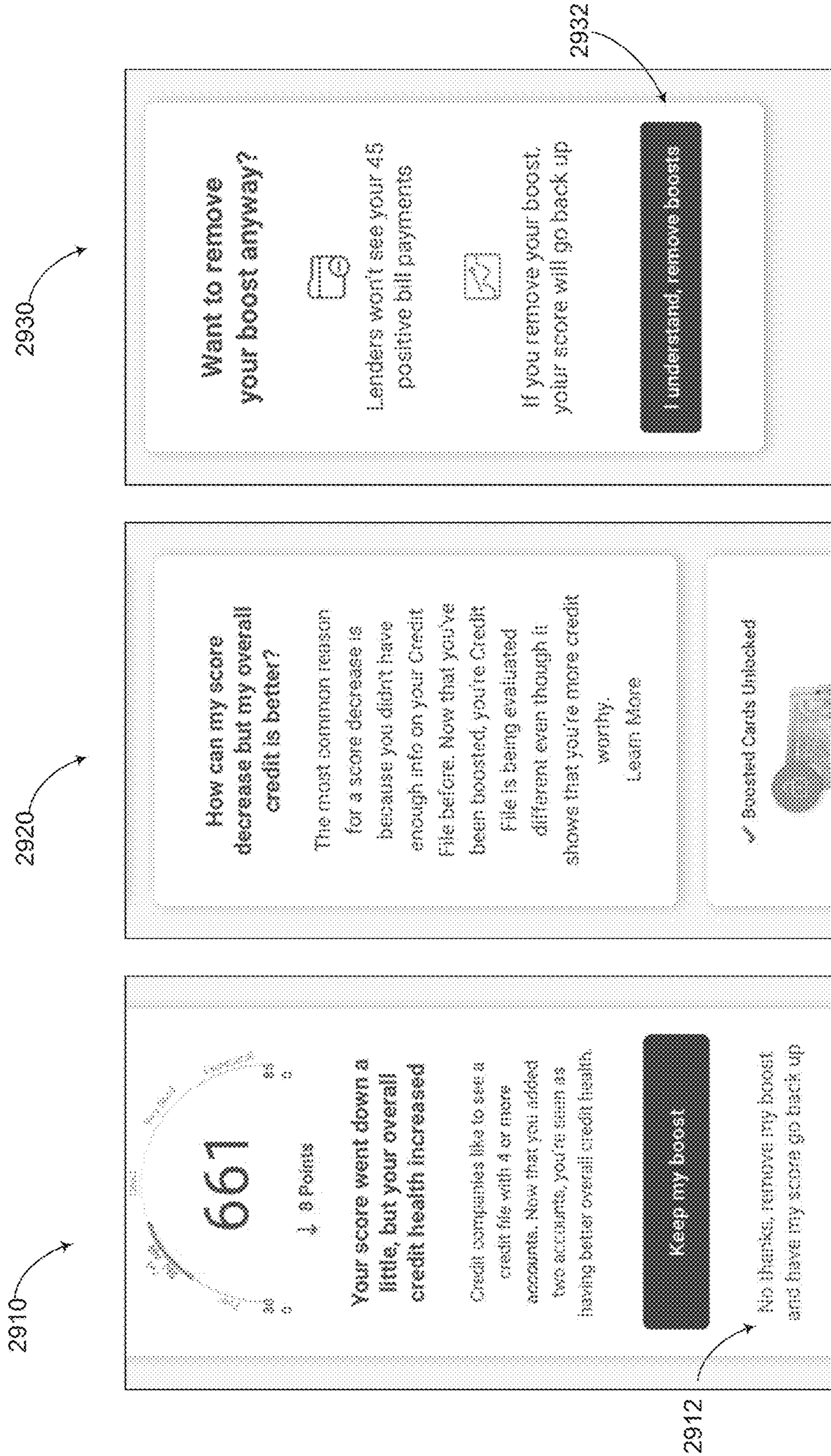


FIGURE 29

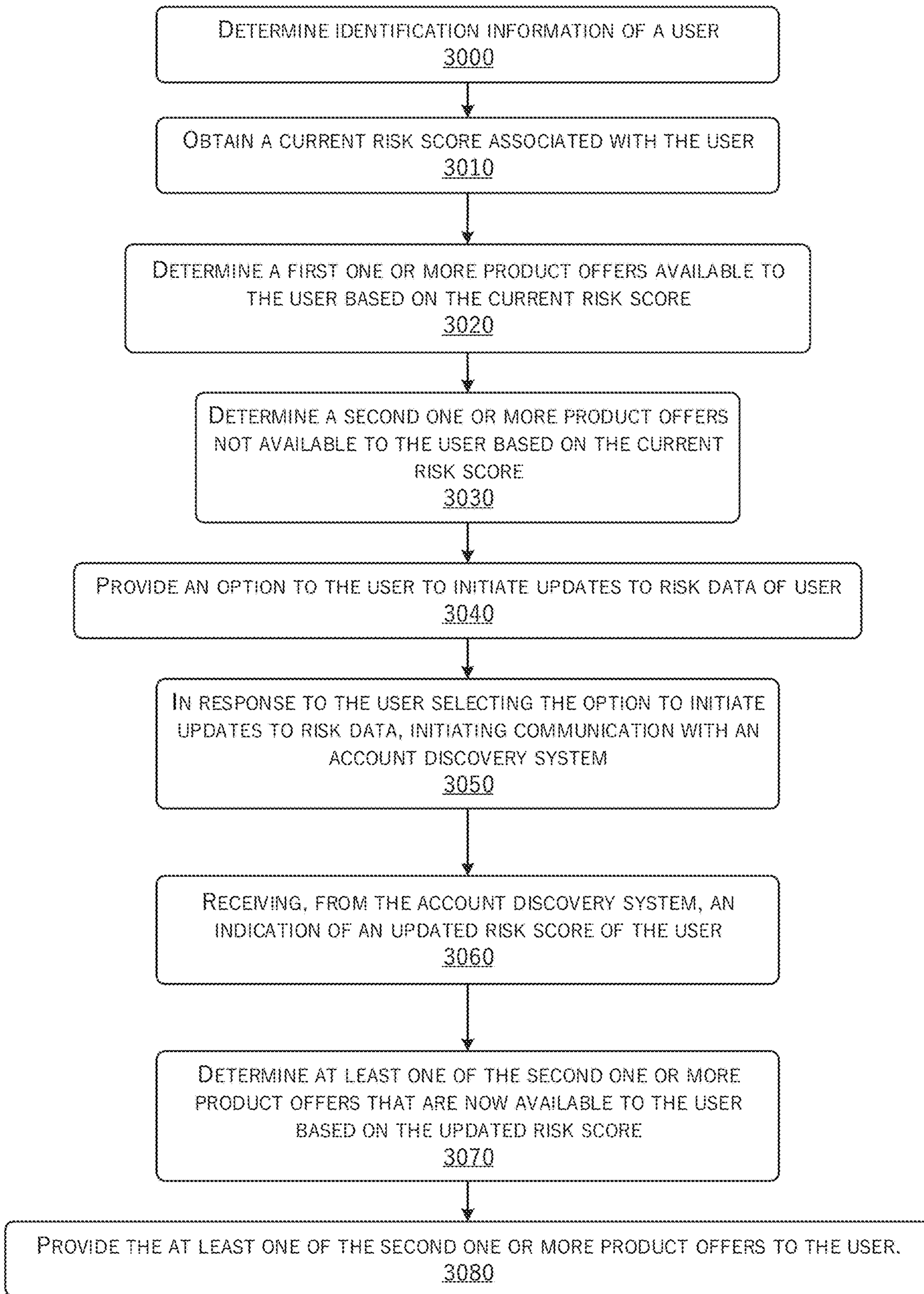


FIGURE 30

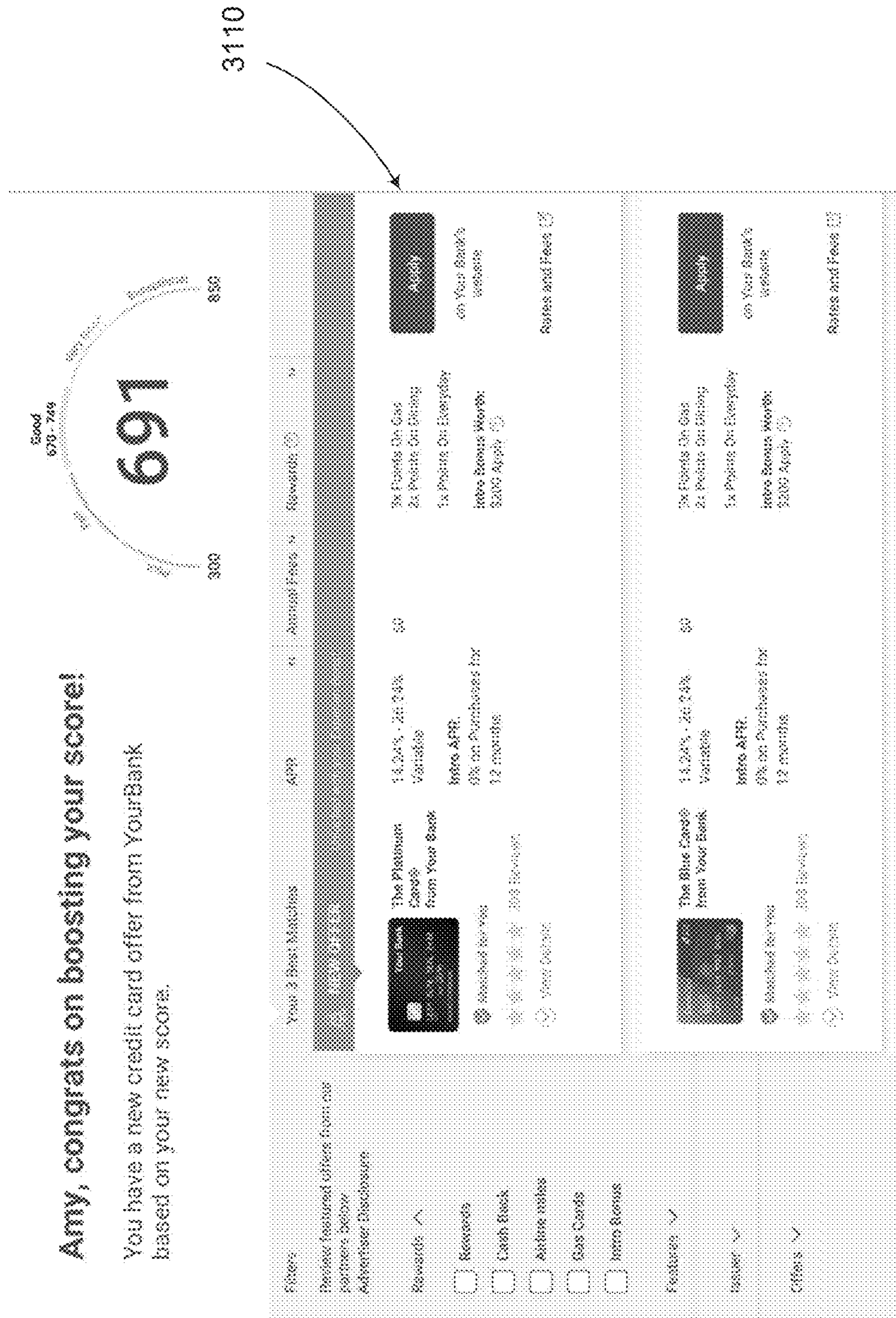


FIGURE 31

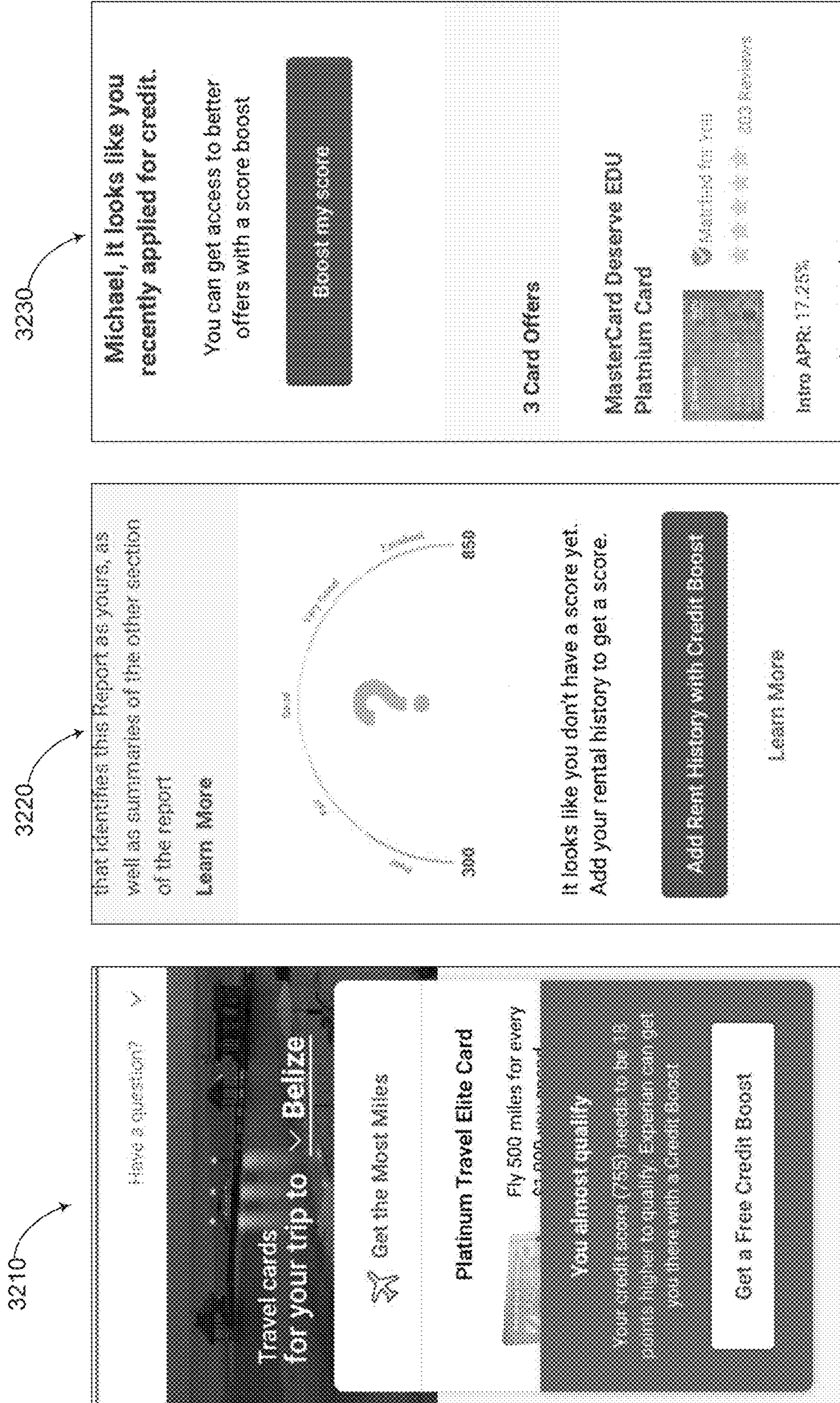


FIGURE 32

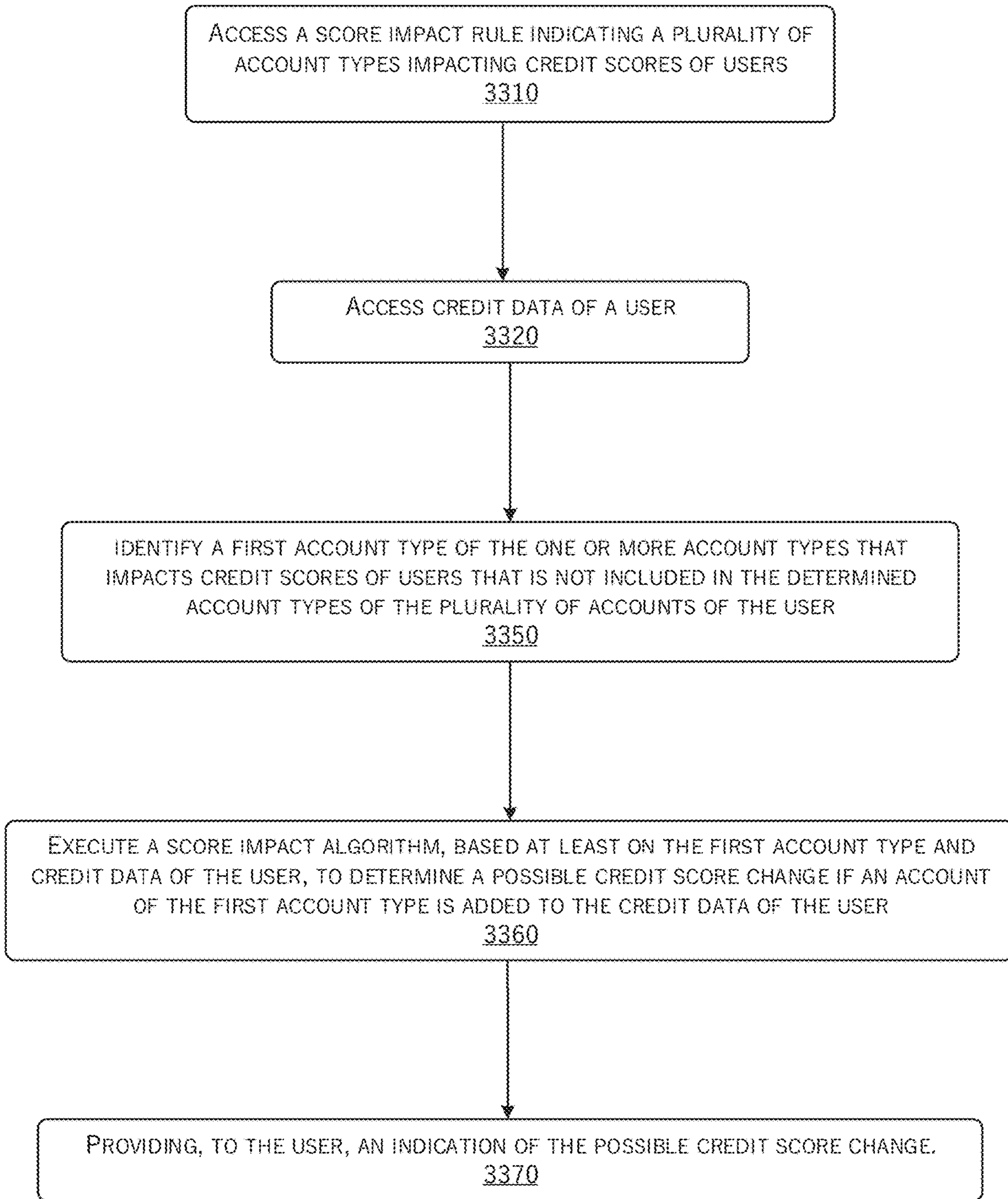


FIGURE 33

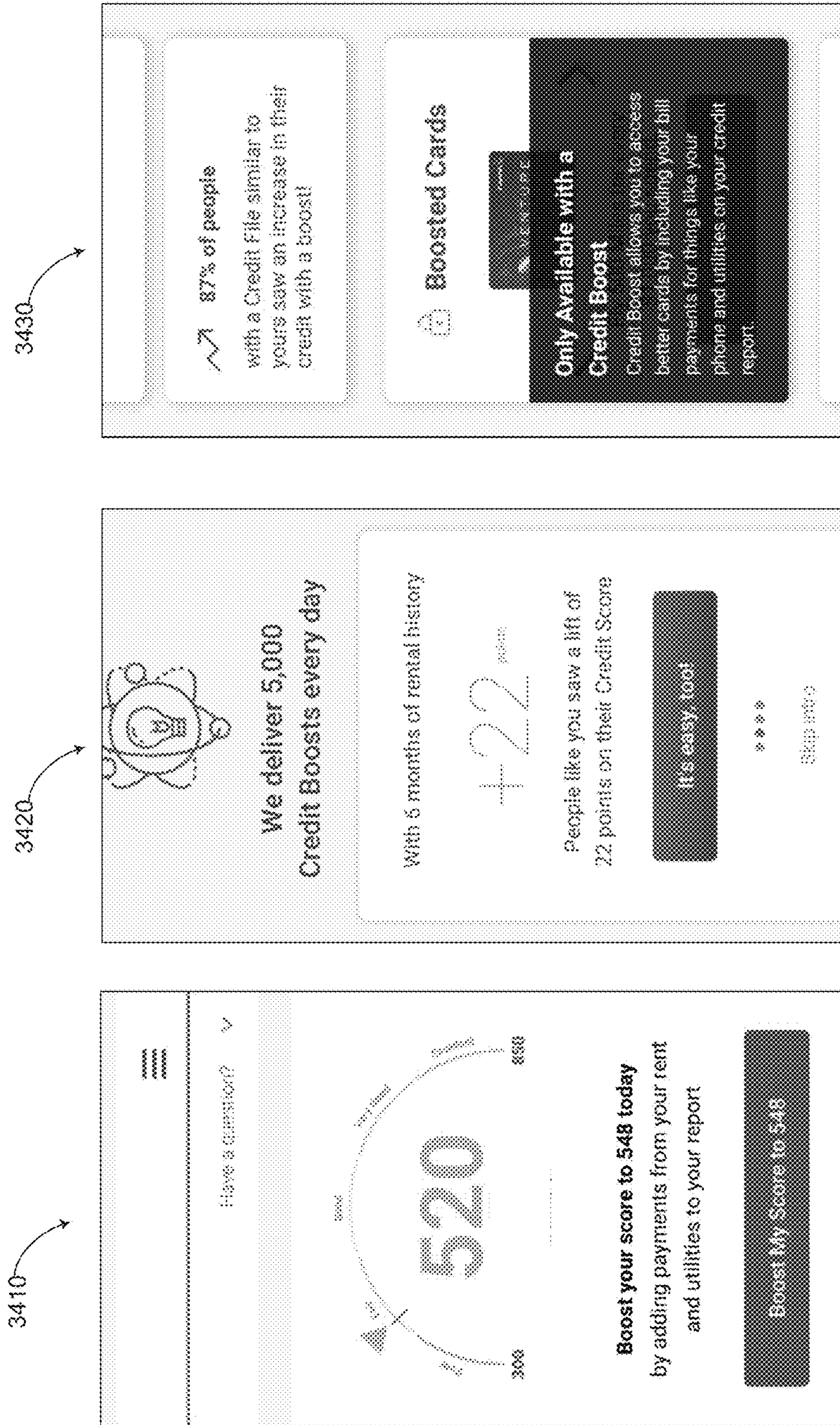
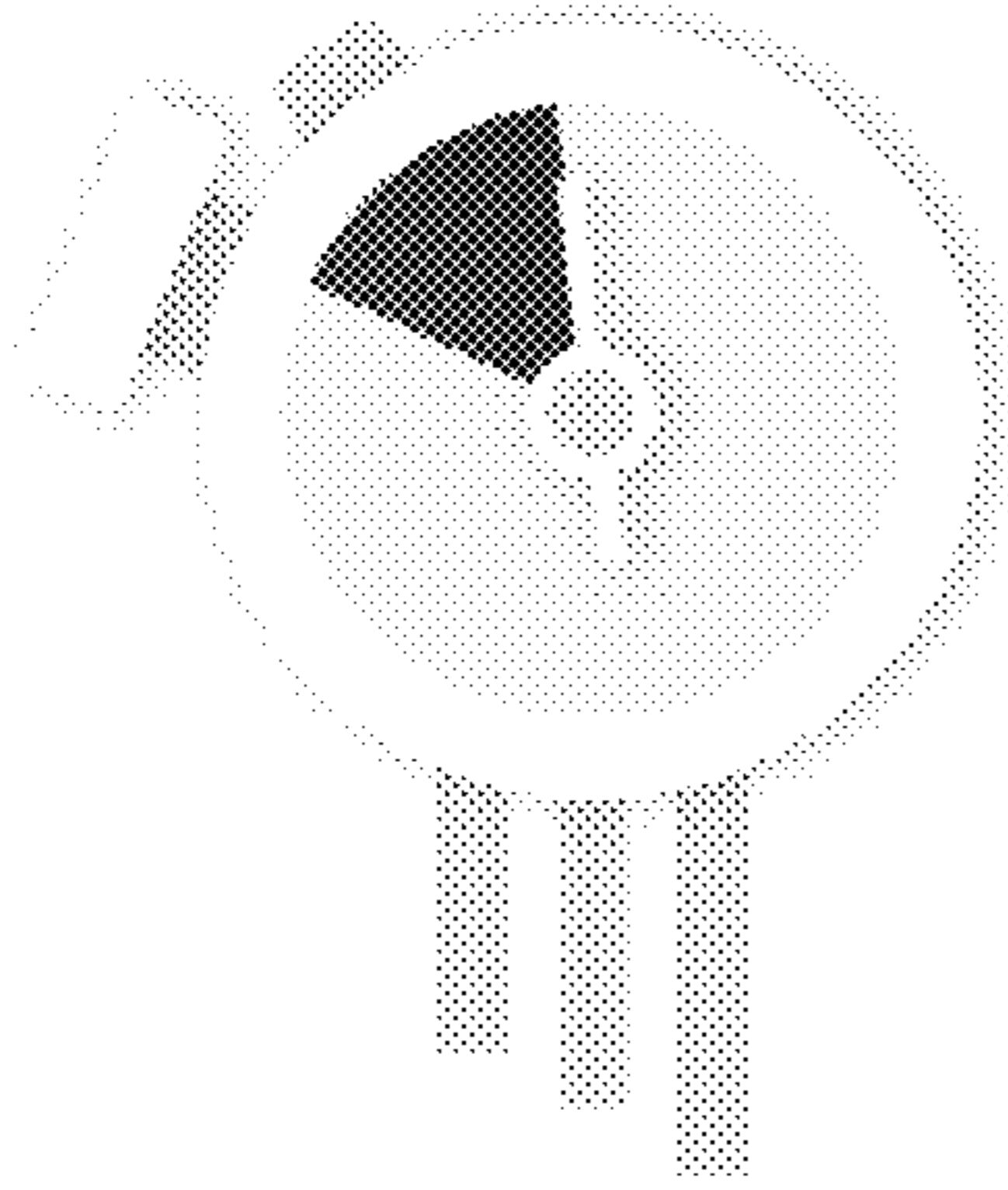


FIGURE 34

X



**85% of people with credit similar to yours
saw an 11 point boost the same day**

Continue >

Those who received an 8 point boost added a
phone bill and two utility bills.

◆ ◆ ◆ ◆
Skip intro, start my boost!

FIGURE 35

3610

X

Do you want to stop reporting So Calif Edison to your Credit File?

- We will no longer add new payments to this account on your credit file
- Your history of 21 positive payments will be deleted from your file
- You won't receive an ongoing boost to your credit from this account
- This may impact your Credit Score
- Keep the 21 positive payments on my MySureau Credit File

Note: This account will be completely removed from your MySureau Credit File

Remove this account

FIGURE 36

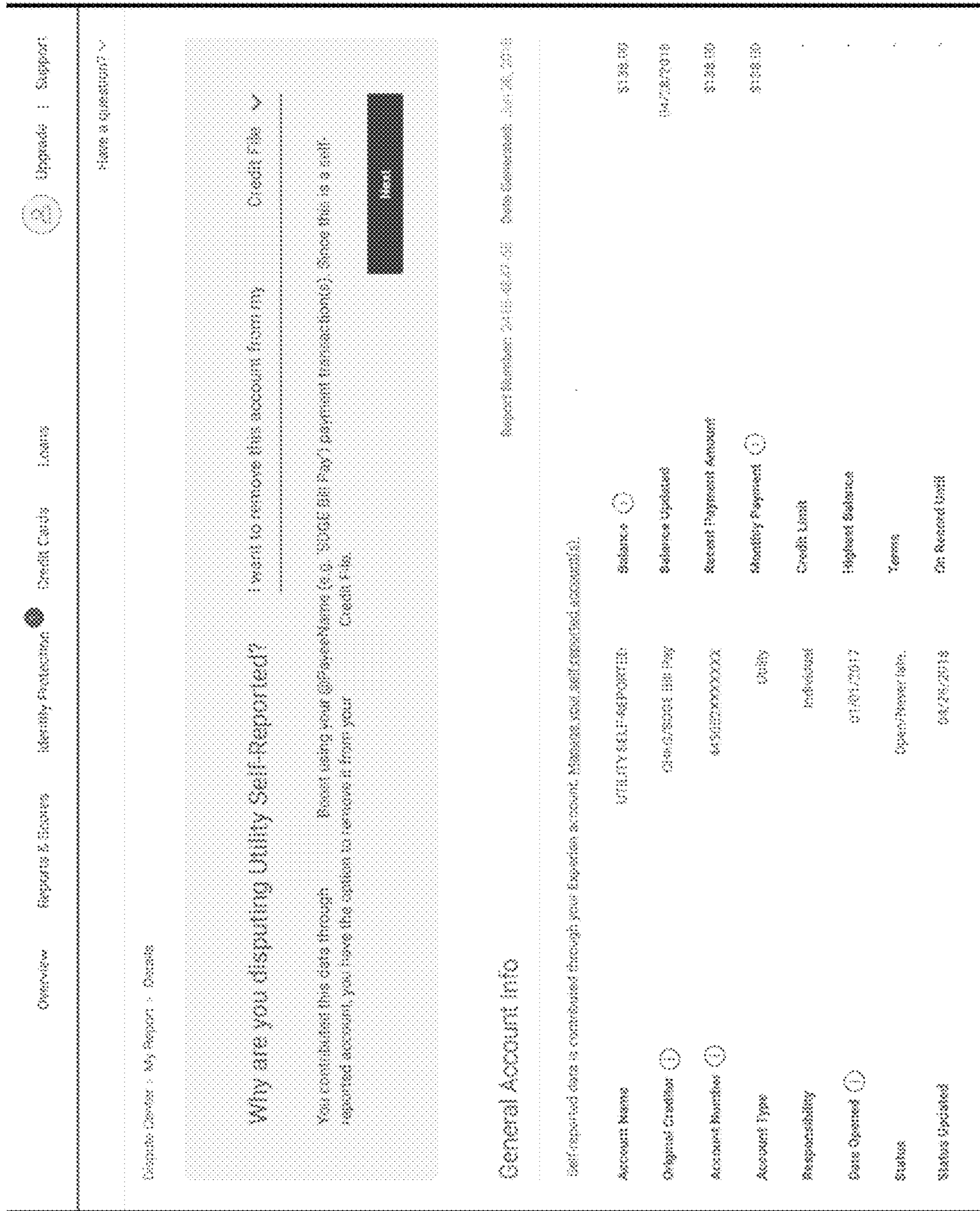


FIGURE 37

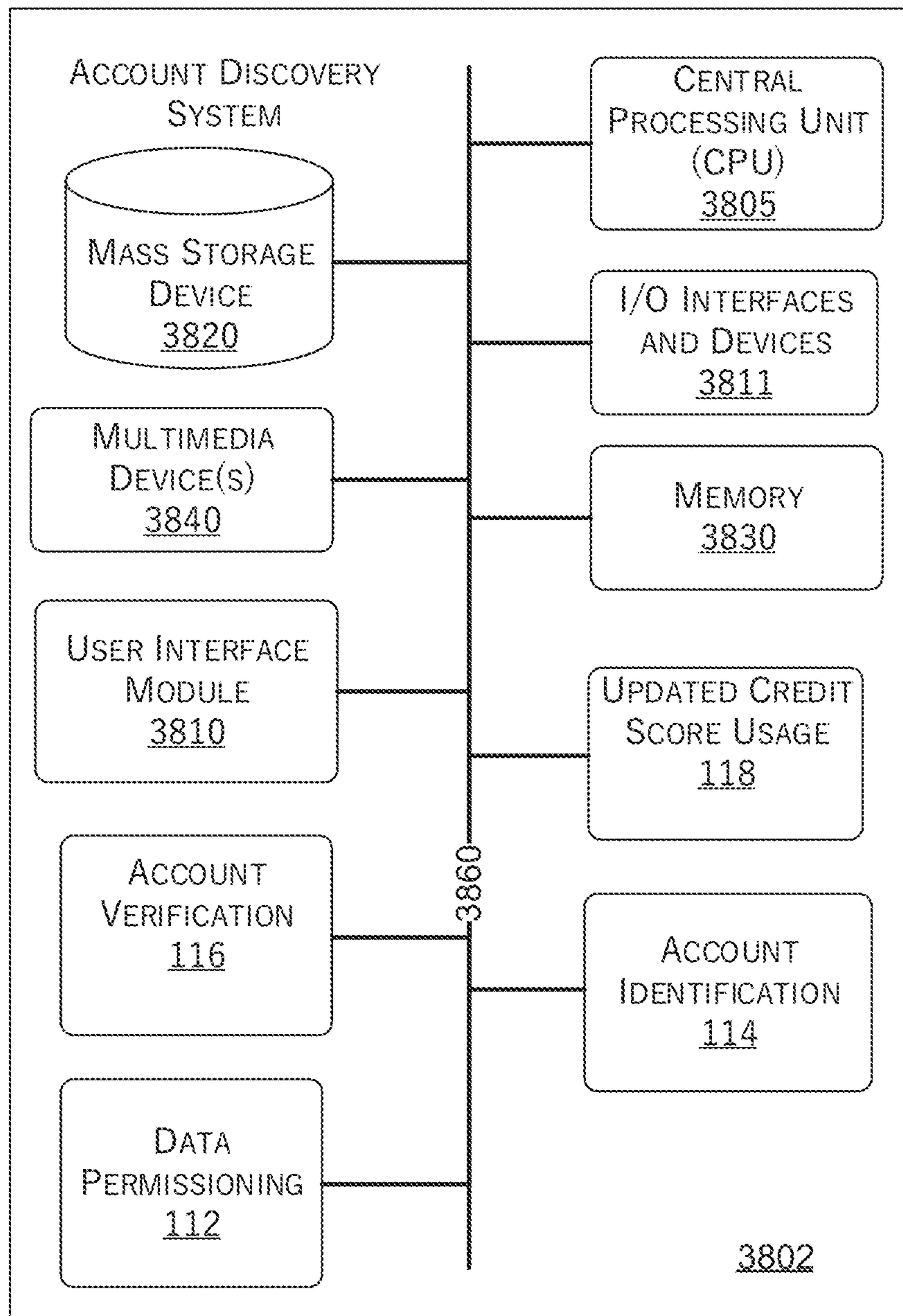


FIGURE 38

USER PERMISSIONS FOR ACCESS TO SECURE DATA AT THIRD-PARTY

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to U.S. patent application Ser. No. 16/445,808 filed on Jun. 19, 2019, which claims priority to U.S. Provisional Patent Application No. 62/727,479 filed on Sep. 5, 2018 and U.S. Provisional Patent Application No. 62/826,319 filed on Mar. 29, 2019, the entire contents of each of which are hereby incorporated herein by reference in their entirety.

LIMITED COPYRIGHT AUTHORIZATION

A portion of the disclosure of this patent document includes material which is subject to copyright protection. The copyright owner has no objection to the facsimile reproduction by anyone of the patent document or the patent disclosure as it appears in the Patent and Trademark Office patent file or records, but otherwise reserves all copyrights whatsoever.

BACKGROUND

Electronic databases provide storage and retrieval of digital data records. Data records in such databases may be electronically updated. Certain data records have access restrictions, such as restrictions regarding entities that can view or make use of the records, as well as restrictions on entities that can provide updates or changes to such records.

SUMMARY OF EMBODIMENTS

The systems, methods, and devices described herein each have several aspects, no single one of which is solely responsible for its desirable attributes. Without limiting the scope of this disclosure, several non-limiting features will now be described briefly.

In some embodiments, an account discovery system interfaces between an end-user (for example, a consumer) and one or more external accounts of the user to identify accounts of the user based on data items accessed at the external accounts. Multiple data items, which may be accessed or received from one or more third-party entities, such as via a direct application programming interface (API) communication channel, are analyzed to determine whether any of the data items, or combinations of data items, meet rules for addition of the data items to a secure third-party risk item database.

A system of one or more computers can be configured to perform particular operations or actions by virtue of having software, firmware, hardware, or a combination of them installed on the system that in operation causes or cause the system to perform the actions. One or more computer programs can be configured to perform particular operations or actions, such as those described below as computerized methods or simply methods, by virtue of including instructions that, when executed by data processing apparatus, cause the apparatus to perform the actions.

In one embodiment, a computerized method is performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system to perform the computerized method comprising receiving, via network com-

munication with a user computing device, selection of a third-party entity from a plurality of third-party entities indicated in a user interface displayed on the user computing device, and credentials for directly accessing, by proxy on behalf of the user via an application programming interface (API), a plurality of data items associated with the user stored in one or more databases associated with the selected third-party entity. The method may further include transmitting at least an API token associated with the selected third-party and the credential to one or more databases associated with the selected third-party, accessing a plurality of data items associated with the user, via an API communication channel established with the one or more databases associated with the selected third-party entity. The method may further include selecting a first data item of the plurality of data items, determining a recipient identified in the first data item, identifying a subset of data items each indicating the determined recipient, wherein the subset of data items includes at least the first data item and one or more other data items. The method may further include determining, based at least on the identified subset of data items, account data associated with an account of the user associated with the recipient, the account data comprising at least one or more of: a number of data items each having time stamps within a predetermined time period, average number of days between time stamps of sequential data items, applying a first account identification rule, associated with a first account type, to the account data, determine, based on said application of the first account identification rule, a first confidence level indicating likelihood that the account is the first type of account. The method may further include, in response to determining that the first confidence level is about a first threshold, applying a first account scoring model to the account data, the first account scoring model configured to determine an expected change to a risk score associated with the user. The method may further include receiving, from the user computing device, confirmation that the account of the user is the first type of account, receiving, from the user computing device, a request to add the account with the recipient to risk data associated with the user at a secured third-party risk database. The method may further include generating, based on portions of the plurality of data items and the account data associated with the recipient, an account creation data package, the account creation data package formatted for ingestion at the secured third-party risk database to initiate addition of the account to risk data of the user, identifying a security key associated with the secured third-party risk database. The method may further include transmitting the security key and the account creation data package to the third-party risk database via a secure communication channel established with the third-party risk database, requesting execution of a risk scoring algorithm using risk data of the user at the secured third-party risk database, wherein the risk scoring algorithm is based at least partly on portions of the plurality of data items or the account data included in the risk data of the user. The method may further include providing risk score change information to the user computing device.

In one embodiment, the method further includes, prior to receiving credentials from the user computing device, transmit user interface data to the user computing device, the user interface data configured to depict a permissions interface element that is selectable to indicate authorization to access account information associated with the user, and receiving, from the user computing device, authorization to access account information associated with the user.

In one embodiment, the method further includes transmitting user interface data to the user computing device, the user interface data configured to depict a user interface including one or more interactive elements selectable to indicate authorized uses of the data items associated with the user by the computing system, receiving, from the user computing device, selection of authorized uses of the data items, and selectively sharing, based on the authorized uses of the data items, the data items with one or more third parties.

In one embodiment, determining a recipient identified in the first data items comprises: determining a recipient identifier in the first data item, accessing a recipient data structure storing indications of associations between recipient identifiers and corresponding recipients, wherein the recipient is associated with a plurality of recipient identifiers used by different third-party databases to identify the recipient, and determining that the recipient identifier is associated with the recipient in the recipient data structure. In one embodiment, associations between recipient identifiers and corresponding recipients are deterministic. In one embodiment, associations between recipient identifiers and corresponding recipients are probabilistic.

In one embodiment, the account creation data package includes at least: an identifier of the recipient, a data furnisher identifier associated with an entity that provides consumer data to the secured third-party risk database, and at least a portion of the account information formatted for ingestion by the secured third-party risk database to initiate addition of the account to risk data of the user. In one embodiment, the security key comprises an API token associated with the secured third-party risk database.

In one embodiment, the method further includes determining a first one or more items available to the user based on the current risk score, determining a second one or more items not available to the user based on the current risk score, determining an estimated risk score of the user based on potential addition of a new account of the user to risk data of the user, in response to determining that at least one of the second one or more items would be available to the user based on the estimated risk score, providing an option to the user in the interactive user interface to initiate updates to risk data of the user, in response to receiving an indication of selection of the option in the interactive user interface on the user device, initiating receiving via network communication with the user computing device, determining an updated risk score based at least on the risk score change information, determining at least one of the second one or more items eligible to the user based on the updated risk score, and updating the interactive user interface data to depict information regarding the at least one of the second one or more items in the user interface on the user device. In one embodiment, the first account scoring model is configured to determine an estimated risk score change if the first account of the first account type is added to the risk data of the user, wherein the first account scoring model is based at least on actual risk score changes of a plurality of other users in response to addition of accounts of the first account type to their respective risk data. In one embodiment, the method further includes, for each of a plurality of accounts included in the risk data of the user, determining an account type from a plurality of account types, identifying a second account type of the plurality of account types that impacts risk scores of users that is not included in the determined account types of the plurality accounts of the user, executing a score impact algorithm, based at least on the second account type and the risk data of the user, to determine a possible risk

score change if an account of the second account type is added to the risk data of the user, and providing, to the user, an indication of the possible risk score change prior to receiving the request to add the account with the recipient to risk data of the user at the secured third-party risk database.

In one embodiment, a computing system comprising a hardware computer processor is configured to perform processor-executable instructions comprising receiving, via network communication with a user computing device, selection of a third-party entity from a plurality of third-party entities indicated in a user interface displayed on the user computing device, and credentials for directly accessing, by proxy on behalf of the user via an application programming interface (API), a plurality of data items associated with the user stored in one or more databases associated with the selected third-party entity, transmitting at least an API token associated with the selected third-party and the credential to one or more databases associated with the selected third-party, accessing a plurality of data items associated with the user, via an API communication channel established with the one or more databases associated with the selected third-party entity, selecting a first data item of the plurality of data items, determining a recipient identified in the first data item, identifying a subset of data items each indicating the determined recipient, wherein the subset of data items includes at least the first data item and one or more other data items, determining, based at least on the identified subset of data items, account data associated with an account of the user associated with the recipient, the account data comprising at least one or more of: a number of data items each having time stamps within a predetermined time period, and average number of days between time stamps of sequential data items. In one embodiment, the operations further comprise applying a first account identification rule, associated with a first account type, to the account data; determining, based on said application of the first account identification rule, a first confidence level indicating likelihood that the account is the first type of account, in response to determining that the first confidence level is about a first threshold, applying a first account scoring model to the account data, the first account scoring model configured to determine an expected change to a current risk score associated with the user, receiving, from the user computing device, confirmation that the account of the user is the first type of account, receiving, from the user computing device, a request to add the account with the recipient to risk data associated with the user at a secured third-party risk database, generating, based on portions of the plurality of data items and the account data associated with the recipient, an account creation data package, the account creation data package formatted for ingestion at the secured third-party risk database to initiate addition of the account to risk data of the user, identifying a security key associated with the secured third-party risk database, transmitting the security key and the account creation data package to the third-party risk database via a secure communication channel established with the third-party risk database, requesting execution of a risk scoring algorithm using risk data of the user at the secured third-party risk database, wherein the risk scoring algorithm is based at least partly on portions of the plurality of data items or the account data included in the risk data of the user, and providing risk score change information to the user computing device.

In one embodiment, the operations further comprise, prior to receiving credentials from the user computing device, transmit user interface data to the user computing device, the user interface data configured to depict a permissions inter-

5

face element that is selectable to indicate authorization to access account information associated with the user, and receiving, from the user computing device, authorization to access account information associated with the user. In one embodiment, the operations further comprise transmitting user interface data to the user computing device, the user interface data configured to depict a user interface including one or more interactive elements selectable to indicate authorized uses of the data items associated with the user by the computing system, receiving, from the user computing device, selection of authorized uses of the data items, and selectively sharing, based on the authorized uses of the data items, the data items with one or more third parties.

In one embodiment, a non-transitory computer readable medium has processor-executable instructions stored thereon that are executable by a hardware computer processor to perform operations comprising receiving, via network communication with a user computing device, selection of a third-party entity from a plurality of third-party entities indicated in a user interface displayed on the user computing device, and credentials for directly accessing, by proxy on behalf of the user via an application programming interface (API), a plurality of data items associated with the user stored in one or more databases associated with the selected third-party entity, transmitting at least an API token associated with the selected third-party and the credential to one or more databases associated with the selected third-party, accessing a plurality of data items associated with the user, via an API communication channel established with the one or more databases associated with the selected third-party entity, selecting a first data item of the plurality of data items, determining a recipient identified in the first data item, identifying a subset of data items each indicating the determined recipient, wherein the subset of data items includes at least the first data item and one or more other data items, determining, based at least on the identified subset of data items, account data associated with an account of the user associated with the recipient, the account data comprising at least one or more of: a number of data items each having time stamps within a predetermined time period, and average number of days between time stamps of sequential data items. In one embodiment, the operations further comprise applying a first account identification rule, associated with a first account type, to the account data; determining, based on said application of the first account identification rule, a first confidence level indicating likelihood that the account is the first type of account, in response to determining that the first confidence level is about a first threshold, applying a first account scoring model to the account data, the first account scoring model configured to determine an expected change to a current risk score associated with the user, receiving, from the user computing device, confirmation that the account of the user is the first type of account, receiving, from the user computing device, a request to add the account with the recipient to risk data associated with the user at a secured third-party risk database, generating, based on portions of the plurality of data items and the account data associated with the recipient, an account creation data package, the account creation data package formatted for ingestion at the secured third-party risk database to initiate addition of the account to risk data of the user, identifying a security key associated with the secured third-party risk database, transmitting the security key and the account creation data package to the third-party risk database via a secure communication channel established with the third-party risk database, requesting execution of a risk scoring algorithm using risk data of the user at the secured third-

6

party risk database, wherein the risk scoring algorithm is based at least partly on portions of the plurality of data items or the account data included in the risk data of the user, and providing risk score change information to the user computing device.

In one embodiment, a non-transitory computer readable medium has processor-executable instructions stored thereon that are executable by a hardware computer processor to perform operations comprising transmitting user interface data to a user computing device, the user interface data configured to depict a permissions interface element that is selectable to indicate authorization to access account information associated with the user, receiving, from the user computing device, authorization to access account information associated with the user, in response to receiving the authorization to access account information associated with the user, receiving, from the user computing device, selection of a third-party entity from a plurality of third-party entities indicated in a user interface on the user computing device, receiving credentials for accessing account information associated with the user at the selected third-party entity, identifying an API token associated with the selected third-party entity, transmitting to an online address associated with a system in electronic communication with the selected third-party entity, the API token and the credentials, receiving, via the system, indicators of one or more accounts of the user with the selected third-party entity, receiving, from the user computing device, selection of an account of the one or more financial accounts, accessing, via a secure communication session initiated with the API token, a plurality of data items of the selected account of the user at the third-party entity, transmitting user interface data to the user computing device, the user interface data configured to depict a user interface on a display of the user computing device, the user interface including one or more interactive elements selectable to indicate authorized uses of the data items by the computing system, receiving, from the user computing device, selection of authorized uses of the data items, and selectively sharing, based on the authorized uses of the data items, the data items with one or more third parties.

In one embodiment, a computerized method performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system comprises transmitting user interface data to a user computing device, the user interface data configured to depict a permissions interface element that is selectable to indicate authorization to access account information associated with the user, receiving, from the user computing device, authorization to access account information associated with the user. The method may further include, in response to receiving the authorization to access account information associated with the user, receiving, from the user computing device, selection of a third-party entity from a plurality of third-party entities indicated in a user interface on the user computing device, receiving credentials for accessing account information associated with the user at the selected third-party entity, identifying an API token associated with the selected third-party entity, transmitting to an online address associated with a system in electronic communication with the selected third-party entity, the API token and the credentials, receiving, via the system, indicators of one or more accounts of the user with the selected third-party entity, receiving, from the user computing device, selection of an account of the one or more financial accounts, accessing, via a secure communication

session initiated with the API token, a plurality of data items of the selected account of the user at the third-party entity, transmitting user interface data to the user computing device, the user interface data configured to depict a user interface on a display of the user computing device, the user interface including one or more interactive elements selectable to indicate authorized uses of the data items by the computing system, receiving, from the user computing device, selection of authorized uses of the data items. The method may further include selectively sharing, based on the authorized uses of the data items, the data items with one or more third parties.

In one embodiment, transaction data items associated with a post date more than one year prior to a current date are disregarded. In one embodiment, transaction data items associated with a post date more than two years prior to a current date are disregarded. In one embodiment, the computing system comprises the system in electronic communication with the selected third-party. In one embodiment, the system in electronic communication with the selected third-party entity is operated by a third-party. In one embodiment, the user interface includes an iframe provided by the system in electronic communication with the selected third-party, wherein the credentials are provided directly to the system electronic communication with the selected third-party. In one embodiment, the credentials are not stored by the computing system. In one embodiment, the credentials comprises a username and password. In one embodiment, the credentials comprise biometric data of the user. In one embodiment, the system in electronic communication with the selected third-party entity communicates with the third-party entity via a secured API communication channel initiated via use of a second API token associated with the third-party entity. In one embodiment, the system in electronic communication with the selected third-party entity stores the credentials for use in a later request for information associated with the user from the selected third-party entity.

In one embodiment, a computerized method performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system comprises receiving, from a user computing device, a request to update risk data of the user with account information regarding an account identified in account data items associated with the user stored by a third-party entity, generating an account creation data package formatted for ingestion at a secured third-party risk database to initiate addition of the account to risk data of the user. The account creation data package may include an identifier of recipient indicated in each of the account data items, a data furnisher identifier associated with an entity that provides consumer data to the secured third-party risk database, and at least a portion of the account information formatted for ingestion by the secured third-party risk database to initiate addition of the account to risk data of the user, identifying an API token associated with the secured third-party risk database. The method may include transmitting the API token and the account creation data package to the secured third-party risk database via an secure communication channel established with the third-party risk database, wherein the account information is usable to update a risk score of the user.

In one embodiment, the account information includes a plurality of historical transaction data items indicating a corresponding plurality of historical transactions between the recipient and the user. In one embodiment, the method

further includes requesting execution of a risk scoring algorithm using risk data of the user at the secured third-party risk database, including the plurality of historical transaction data items included in the risk data of the user. In one embodiment, the method further includes receiving, from the secured third-party risk database, a risk score of the user based on said execution of the risk scoring algorithm, and transmitting a notification to the user indicating the risk score. In one embodiment, the method further includes, in response to determining that the risk score is lower than a previous risk score of the user, initiating activation of a user interface on the user computing device that includes an option to remove the account information from the risk data of the user, in response to selection of the option to remove the account information from the risk data of the user, generating an account removal data package formatted for ingestion at the secured third-party risk database to initiate removal of the account from risk data of the user, the account removal data package including: the identifier of the recipient and the data furnisher identifier associated with the entity that provides consumer data to the secured third-party risk database, and transmitting the account removal data package to the secured third-party risk database via a secure communication channel.

In one embodiment, the method further includes receiving updated account information regarding the account associated with the user, the updated account information including a transaction data item not included in the plurality of historical transaction data items, generating an account update data package formatted for ingestion at the secured third-party risk database to initiate update of risk data of the user associated with the account, the account update data package including: an identifier of the recipient indicated in the transaction data item, the data furnisher identifier associated with the entity that provides consumer data to the secured third-party risk database, and at least a portion of the updated account information formatted for ingestion by the secured third-party risk database to initiate addition of the transaction data item to risk data of the user, and transmitting the API token associated with the secured third-party risk database and the account update data package to the secured third-party risk database. In one embodiment, the method further includes, requesting execution of a risk scoring algorithm using risk data of the user at the secured third-party risk database, wherein the risk scoring algorithm is based at least partly on portions of the plurality of historical transaction data items and the transaction data item. In one embodiment, the method further includes receiving, from the secured third-party risk database, a risk score of the user based on said execution of the risk scoring algorithm, and in response to determining that a risk score of the user is different than prior to transmitting the account update data package to the secured third-party risk database, transmitting a notification to the user. In one embodiment, the notification comprises a push notification to the user computing device, the push notification configured to automatically activate an application on the user computing device to cause display of information associated with the notification. In one embodiment, the notification is transmitted to the user in real-time from receiving the updated account information.

In one embodiment, the computerized method further comprises receiving, via network communication with the user computing device, selection of a third-party entity from a plurality of third-party entities indicated in a user interface displayed on the user computing device, credentials for directly accessing, by proxy on behalf of the user via an application programming interface (API), the account items

associated with the user stored in one or more databases associated with the third-party entity, transmitting at least an API token associated with the selected third-party and the credential to one or more databases associated with the selected third-party entity, accessing the account data items associated with the user, via an API communication channel established with the one or more databases associated with the selected third-party entity, selecting a first data item of the plurality of account data items, determining a recipient identified in the first data item, identifying a subset of account data items each indicating the determined recipient, wherein the subset of account data items includes at least the first data item and one or more other account data items, determining, based at least on the identified subset of account data items, account data associated with an account of the user associated with the recipient, the account data comprising at least one or more of: a number of account data items each having time stamps within a predetermined time period, and average number of days between time stamps of sequential account data items, applying a first account identification rule, associated with a first account type, to the account data, determine, based on said application of the first account identification rule, a first confidence level indicating likelihood that the account is the first type of account. In some embodiments, the method further includes, in response to determining that the first confidence level is above a first threshold, applying a first account scoring model to the account data, the first account scoring model configured to determine an expected change to a current risk score associated with the user, requesting execution of a risk scoring algorithm using risk data of the user at the secured third-party risk database, wherein the risk scoring algorithm is based at least partly on portions of the plurality of account data items or the account data included in the risk data of the user, and providing risk score change information to the user computing device.

In one embodiment, a computing system comprising a hardware computer processor is configured to perform operations comprising receiving, from a user computing device, a request to update risk data of the user with account information regarding an account identified in account data items associated with the user stored by a third-party entity, generating an account creation data package formatted for ingestion at a secured third-party risk database to initiate addition of the account to risk data of the user, the account creation data package including: an identifier of recipient indicated in each of the account data items, a data furnisher identifier associated with an entity that provides consumer data to the secured third-party risk database, and at least a portion of the account information formatted for ingestion by the secured third-party risk database to initiate addition of the account to risk data of the user. In some embodiments, the operations further include identifying an API token associated with the secured third-party risk database and transmitting the API token and the account creation data package to the secured third-party risk database via a secure communication channel established with the third-party risk database, wherein the account information is usable to update a risk score of the user.

In one embodiment, the account information includes a plurality of historical transaction data items indicating a corresponding plurality of historical transactions between the recipient and the user. In one embodiment, the operations further comprise requesting execution of a risk scoring algorithm using risk data of the user at the secured third-party risk database, including the plurality of historical transaction data items included in the risk data of the user.

In one embodiment, the operations further comprise receiving, from the secured third-party risk database, a risk score of the user based on said execution of the risk scoring algorithm and transmitting a notification to the user indicating the risk score.

In one embodiment, a non-transitory computer readable medium having processor-executable instructions stored thereon that are executable by a hardware computer processor to perform operations comprising receiving, from a user computing device, a request to update risk data of the user with account information regarding an account identified in account data items associated with the user stored by a third-party entity, generating an account creation data package formatted for ingestion at a secured third-party risk database to initiate addition of the account to risk data of the user, the account creation data package including: an identifier of recipient indicated in each of the account data items, a data furnisher identifier associated with an entity that provides consumer data to the secured third-party risk database, and at least a portion of the account information formatted for ingestion by the secured third-party risk database to initiate addition of the account to risk data of the user. In one embodiment, the operations further comprise identifying an API token associated with the secured third-party risk database, and transmitting the API token and the account creation data package to the secured third-party risk database via a secure communication channel established with the third-party risk database, wherein the account information is usable to update a risk score of the user.

In one embodiment, a computerized method performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system comprises receiving authentication information from a user computing device, the authentication information including at least a name and address of a user, transmitting, to a secured third-party risk system, a request for execution of a risk scoring algorithm to determine a current risk score of the user based at least on risk data of the user at the secured third-party risk system, receiving, from the secured third-party risk system, the current risk score of the user, accessing an item database including information associated with a plurality of items and, for each item, an associated criteria for matching the item with users, querying the item database with at least the current risk score of the user, receiving, in response to said querying the item database, information indicating: a first one or more items matched to the user based on the current risk score, and a second one or more items not matched to the user based on the current risk score. In one embodiment, the method further comprises generating interactive user interface data configured to display an interactive user interface on the user computing device, the user interface depicting information regarding at least one of the first one or more items, determining an estimated risk score of the user based on potential addition of a new account of the user to risk data of the user, in response to determining that at least one of the second one or more items would be matched to the user based on the estimated risk score, providing an option to the user in the interactive user interface to initiate updates to risk data of the user, in response to receiving an indication of selection of the option in the interactive user interface on the user computing device, initiating communication between the user computing device and an account discovery system, wherein the account discovery system is configured to identify a new account of the user through analysis of data items associated with the user stored by one

or more third-party databases, transmitting, to the secured third-party risk system, a second request for execution of the risk scoring algorithm to determine an updated risk score of the user based at least on risk data of the user, including information regarding the new account of the user, at the secured third-party risk system, receiving, from the secured third-party risk system, the updated risk score of the user, querying the item database with at least the updated risk score of the user, receiving, in response to said querying the item database, information indicating that at least one of the second one or more data items matched to the user based on the updated risk score and updating the interactive user interface data to depict information regarding the at least one of the second one or more items in the user interface on the user computing device.

In one embodiment, the updated risk score equals the estimated risk score. In one embodiment, the user interface further depicts a first access link to a first enrollment entity associated with a first of the one or more items. In one embodiment, the first access link is configured to redirect communication of the user computing device to an enrollment website. In one embodiment, the access links comprise hyperlinks. In one embodiment, said determining the estimated risk score comprises determining a first account type of a plurality of account types that impacts risk scores of users that is not included in risk data of the user, determining a score impact associated with the determined first account type, and calculating the estimated risk score based at least on the current risk score and the score impact. In one embodiment, said determining the score impact associated with the determined first account type comprises identifying a plurality of other users associated with addition of accounts of the first account type to respective risk data, and, based on account data of the plurality of other users, generating a score impact algorithm configured to determine, for respective users, score impacts in response to addition of accounts of the first account type. In one embodiment, the plurality of other users are identified as users having accounts of the first account type with account attributes within a predetermined threshold of account attributes of the new account of the user.

In one embodiment, the method further comprises generating a first access link associated with a first item, the first access link including an online address of a first enrollment entity and personally identifiable information of the user, wherein the personally identifiable information is usable by the first enrollment entity to auto-populate an enrollment user interface with the personally identifiable information of the user. In one embodiment, the items are products or services. In one embodiment, first criteria for matching a first item with users is based on a risk score of the user being greater than a predetermined risk score threshold. In one embodiment, the user interface further includes a filter control configured for interaction with the user of the user computing device to receive a filter criteria, wherein application of the filter criteria generates a filtered set of the first one or more items.

In one embodiment, the account discovery system is configured to perform operations comprising receiving, via network communication with a user computing device, selection of a third-party entity from a plurality of third-party entities indicated in a user interface displayed on the user computing device, credentials for directly accessing, by proxy on behalf of the user via an application programming interface (API), a plurality of data items associated with the user stored in one or more databases associated with the selected third-party entity, transmitting at least an API token

associated with the selected third-party and the credential to one or more databases associated with the selected third-party entity, accessing a plurality of data items associated with the user, via an API communication channel established with the one or more databases associated with the selected third-party entity, selecting a first data item of the plurality of data items, determining a recipient identified in the first data item, identifying a subset of data items each indicating the determined recipient, wherein the subset of data items includes at least the first data item and one or more other data items, determining, based at least on the identified subset of data items, account data associated with an account of the user associated with the recipient, the account data comprising at least one or more of: a number of data items each having time stamps within a predetermined time period, and an average number of days between time stamps of sequential data items, applying a first account identification rule, associated with a first account type, to the account data, determine, based on said application of the first account identification rule, a first confidence level indicating likelihood that the account is the first type of account. In one embodiment, the method further includes, in response to determining that the first confidence level is above a first threshold, applying a first account scoring model to the account data, the first account scoring model configured to determine an expected change to a current risk score associated with the user, receiving, from the user computing device, confirmation that the account of the user is the first type of account, receiving, from the user computing device, a request to add the account with the recipient to risk data associated with the user at a secured third-party risk database, generating, based on portions of the plurality of data items and the account data associated with the recipient, an account creation data package, the account creation data package formatted for ingestion at the secured third-party risk database to initiate addition of the account to risk data of the user, identifying a security key associated with the secured third-party risk database, and transmitting the security key and the account creation data package to the third-party risk database via a secure communication channel established with the third-party risk database.

In one embodiment, a computing system comprises a hardware computer processor configured to perform operations comprising receiving authentication information from a user computing device, the authentication information including at least a name and address of a user, transmitting, to a secured third-party risk system, a request for execution of a risk scoring algorithm to determine a current risk score of the user based at least on risk data of the user at the secured third-party risk system, receiving, from the secured third-party risk system, the current risk score of the user, accessing an item database including information associated with a plurality of items and, for each item, an associated criteria for matching the item with users, querying the item database with at least the current risk score of the user, receiving, in response to said querying the item database, information indicating: a first one or more items matched to the user based on the current risk score; and a second one or more items not matched to the user based on the current risk score, generating interactive user interface data configured to display an interactive user interface on the user computing device, the user interface depicting information regarding at least one of the first one or more items, determining an estimated risk score of the user based on potential addition of a new account of the user to risk data of the user, in response to determining that at least one of the second one or more items would be matched to the user based on the

estimated risk score, providing an option to the user in the interactive user interface to initiate updates to risk data of the user, in response to receiving an indication of selection of the option in the interactive user interface on the user computing device, initiating communication between the user computing device and an account discovery system, wherein the account discovery system is configured to identify a new account of the user through analysis of data items associated with the user stored by one or more third-party databases, transmitting, to the secured third-party risk system, a second request for execution of the risk scoring algorithm to determine an updated risk score of the user based at least on risk data of the user, including information regarding the new account of the user, at the secured third-party risk system, receiving, from the secured third-party risk system, the updated risk score of the user, querying the item database with at least the updated risk score of the user, receiving, in response to said querying the item database, information indicating that at least one of the second one or more data items matched to the user based on the updated risk score, and updating the interactive user interface data to depict information regarding the at least one of the second one or more items in the user interface on the user computing device.

In one embodiment, the operations further include generating a first access link associated with a first item, the first access link including an online address of a first enrollment entity and personally identifiable information of the user, wherein the personally identifiable information is usable by the first enrollment entity to auto-populate an enrollment user interface with the personally identifiable information of the user.

In one embodiment, a computerized method performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system performs the computerized method comprising determining identification information of a user, obtaining a current risk score associated with the user, determining a first one or more items available to the user based on the current risk score, determining a second one or more items not available to the user based on the current risk score, generating interactive user interface data configured to display an interactive user interface on a user device, the user interface depicting information regarding at least one of the first one or more items, including an access link to an enrollment entity associated with the at least one of the first one or more items, determining an estimated risk score of the user based on potential addition of a new account of the user to risk data of the user, in response to determining that at least one of the second one or more items would be available to the user based on the estimated risk score, providing an option to the user in the interactive user interface to initiate updates to risk data of the user, in response to receiving an indication of selection of the option in the interactive user interface on the user device, initiating communication between the user device and an account discovery system, wherein the account discovery system is configured to identify a new account of the user through analysis of data items associated with the user stored by one or more third-party databases and to trigger generation of an updated risk score, receiving an indication of an updated risk score of the user, wherein the updated risk score is higher than the current risk score based on addition of the new account to risk data of the user by the account discovery system, determining at least one of the second one or more items eligible to the user based on the updated risk score, and

updating the interactive user interface data to depict information regarding the at least one of the second one or more items in the user interface on the user device.

In one embodiment, a non-transitory computer readable medium having processor-executable instructions stored thereon are executable by a hardware computer processor to perform operations comprising receiving authentication information from a user computing device, the authentication information including at least a name and address of a user, transmitting, to a secured third-party risk system, a request for execution of a risk scoring algorithm to determine a current risk score of the user based at least on risk data of the user at the secured third-party risk system, receiving, from the secured third-party risk system, the current risk score of the user, accessing an item database including information associated with a plurality of items and, for each item, an associated criteria for matching the item with users, querying the item database with at least the current risk score of the user, receiving, in response to said querying the item database, information indicating: a first one or more items matched to the user based on the current risk score, and a second one or more items not matched to the user based on the current risk score, generating interactive user interface data configured to display an interactive user interface on the user computing device, the user interface depicting information regarding at least one of the first one or more items, determining an estimated risk score of the user based on potential addition of a new account of the user to risk data of the user, in response to determining that at least one of the second one or more items would be matched to the user based on the estimated risk score, providing an option to the user in the interactive user interface to initiate updates to risk data of the user, in response to receiving an indication of selection of the option in the interactive user interface on the user computing device, initiating communication between the user computing device and an account discovery system, wherein the account discovery system is configured to identify a new account of the user through analysis of data items associated with the user stored by one or more third-party databases, transmitting, to the secured third-party risk system, a second request for execution of the risk scoring algorithm to determine an updated risk score of the user based at least on risk data of the user, including information regarding the new account of the user, at the secured third-party risk system, receiving, from the secured third-party risk system, the updated risk score of the user, querying the item database with at least the updated risk score of the user, receiving, in response to said querying the item database, information indicating that at least one of the second one or more data items matched to the user based on the updated risk score, and updating the interactive user interface data to depict information regarding the at least one of the second one or more items in the user interface on the user computing device.

In one embodiment, a computerized method performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system comprises accessing a score impact rule indicating one or more account types that impacts risk scores of users, identifying an API token associated with a secured third-party risk database, transmitting the API token and a request for risk data of a user to the third-party risk database. The method may include accessing, via an secure communication channel established with the third-party risk database, risk data of the user,

identifying a plurality of groupings of data items (which may also be referred to as subsets of data items) included in the risk data of the user, each of the groupings including a plurality of data items associated with an entity, determining an account type of a plurality of account types for each of the groupings of data items, identifying a first account type of the one or more account types that impacts credit scores of users that is not included in the determined account types of the plurality of groups of data items associated with the user, execute a score impact algorithm, based at least on the first account type and the risk data of the user, to determine a possible risk score change if an account of the first account type is added to the risk data of the user. The method may include providing, to the user, an indication of the possible risk score change.

In one embodiment, the possible risk score changes indicates an estimated risk score. In one embodiment, the possible risk score changes indicates an estimated risk score increase or decrease. In one embodiment, the method further comprises providing, to the user, an option to initiate addition of an account of the first account type to risk data of the user. In one embodiment, a first plurality of data items associated with a second entity indicate transactions of the user in a second account of the second account type. In one embodiment, the score impact algorithm is developed based at least on historical risk score changes of a plurality of other users in response to addition of respective accounts of the first account type to respective risk data of the users. In one embodiment, the method further comprises executing a second score impact algorithm configured to estimate a second possible risk score associated with addition of a second account of a second account type to the risk data of the user, and providing, to the user, a second indication of the second possible risk score change.

In one embodiment, the computerized method of further comprises receiving, via network communication with a user computing device, selection of a third-party entity from a plurality of third-party entities indicated in a user interface displayed on the user computing device, credentials for directly accessing, by proxy on behalf of the user via an application programming interface (API), a plurality of data items associated with the user stored in one or more databases associated with the selected third-party entity, transmitting at least an API token associated with the selected third-party and the credential to one or more databases associated with the selected third-party entity, accessing a plurality of data items associated with the user, via an API communication channel established with the one or more databases associated with the selected third-party entity, wherein said identifying a plurality of groupings of data items further comprises: selecting a first data item of the plurality of data items, determining a recipient identified in the first data item, identifying a subset grouping of data items each indicating the determined recipient, wherein the subset grouping of data items includes at least the first data item and one or more other data items, determining, based at least on the identified subset grouping of data items, account data associated with an account of the user associated with the recipient, the account data comprising at least one or more of: a number of data items each having time stamps within a predetermined time period, and an average number of days between time stamps of sequential data items. In one embodiment, the method further includes applying a first account identification rule, associated with the first account type, to the account data, determine, based on said application of the first account identification rule, a first confidence level indicating likelihood that the account

is the first type of account, in response to determining that the first confidence level is above a first threshold, applying a first account scoring model to the account data, the first account scoring model configured to determine an expected change to a current risk score associated with the user, receiving, from the user computing device, confirmation that the account of the user is the first type of account type, receiving, from the user computing device, a request to add the account with the recipient to risk data associated with of the user at a the secured third-party risk database, generating, based on portions of the plurality of data items and the account data associated with the recipient, an account creation data package, the account creation data package formatted for ingestion at the secured third-party risk database to initiate addition of the account to risk data of the user, identifying a security key associated with the secured third-party risk database, transmitting the security key and the account creation data package to the third-party risk database via a secure communication channel established with the third-party risk database, requesting execution of a risk scoring algorithm using risk data of the user at the secured third-party risk database, wherein the risk scoring algorithm is based at least partly on portions of the plurality of data items or the account data included in the risk data of the user, and providing risk score change information to the user computing device.

In one embodiment, a computing system is configured to perform operations comprising accessing a score impact rule indicating one or more account types that impacts risk scores of users, identifying an API token associated with a secured third-party risk database, transmitting the API token and a request for risk data of a user to the third-party risk database, accessing, via a secure communication channel established with the third-party risk database, risk data of the user, identifying a plurality of groupings of data items included in the risk data of the user, each of the groupings including a plurality of data items associated with an entity, determining, for each of the groupings of data items, an account type of a plurality of account types, identifying a first account type of the plurality of account types that impacts risk scores when added to risk data of respective users and is not included in the determined account types associated with the user, executing a score impact algorithm, based at least on the first account type and the risk data of the user, to determine a possible risk score change if an account of the first account type is added to the risk data of the user, and providing, to the user, an indication of the possible risk score change.

In one embodiment, the possible risk score changes indicates an estimated risk score. In one embodiment, the possible risk score changes indicates an estimated risk score increase or decrease. In one embodiment, the operations further comprise providing, to the user, an option to initiate addition of an account of the first account type to risk data of the user. In one embodiment, a first plurality of data items associated with a second entity indicate transactions of the user in a second account of the second account type. In one embodiment, the score impact algorithm is developed based at least on historical risk score changes of a plurality of other users in response to addition of respective accounts of the first account type to respective risk data of the users. In one embodiment, the operations further comprise executing a second score impact algorithm configured to estimate a second possible risk score associated with addition of a second account of a second account type to the risk data of the user, and providing, to the user, a second indication of the second possible risk score change.

In one embodiment, a non-transitory computer readable medium having processor-executable instructions stored thereon that are executable by a hardware computer processor to perform operations comprising accessing a score impact rule indicating one or more account types that impacts risk scores of users, identifying an API token associated with a secured third-party risk database, transmitting the API token and a request for risk data of a user to the third-party risk database, accessing, via a secure communication channel established with the third-party risk database, risk data of the user, identifying a plurality of groupings of data items included in the risk data of the user, each of the groupings including a plurality of data items associated with an entity, determining, for each of the groupings of data items, an account type of a plurality of account types, identifying a first account type of the plurality of account types that impacts risk scores when added to risk data of respective users and is not included in the determined account types associated with the user, executing a score impact algorithm, based at least on the first account type and the risk data of the user, to determine a possible risk score change if an account of the first account type is added to the risk data of the user, and providing, to the user, an indication of the possible risk score change.

BRIEF DESCRIPTION OF THE FIGURES

FIG. 1 is an embodiment of a flow diagram illustrating example components and example communications between the components of an embodiment of an authenticated access and aggregation database platform.

FIG. 2A is an embodiment of a block diagram illustrating an account discovery system in communication with various external devices and systems via a network.

FIG. 2B is one embodiment of a block diagram illustrating another example embodiment of an account discovery system in communication with various external computing systems and devices.

FIG. 3 is one embodiment of an example user interface that may be provided to a user to initiate an account discovery process.

FIG. 4 is one embodiment of a block diagram illustrating various components and processes that may be performed according to various embodiments discussed herein.

FIG. 5 is an embodiment of a flowchart illustrating one example of a process of interacting with a consumer, accessing DDA account data of the consumer, identifying non-traditional account(s) of the consumer in the DDA account data, and updating credit data of the consumer at a credit bureau.

FIG. 6 is an embodiment of a block diagram illustrating another example of an account access system and an account discovery system in communication with one another (whether operated by a single and the or by separate entities).

FIG. 7 is one embodiment of a flowchart illustrating one example of a method that may be performed to authorize and initiate access to a user's DDA account information at a financial institution.

FIG. 8 illustrates embodiments of three example user interfaces that may be displayed on a user device.

FIG. 9 illustrates embodiments of example user interfaces that may be provided by the data permissioning component, whether operated by a third-party account access system or the account discovery system, to obtain access credentials from the user.

FIG. 10 illustrates an embodiment of an example user interface that may be presented to the user indicating multiple accounts identified at the financial institution, and providing the user an option to select one or more of the accounts from which the account access system will be authorized to access specific transaction data items.

FIG. 11 is an embodiment of a flowchart illustrating one example of a method that may be performed to categorize data items (for example, transaction data items) from the transaction provider (for example, a financial institution).

FIG. 12 is one embodiment of a flowchart illustrating one embodiment of a method for identifying account types of interest from groupings of transaction data items (for example, from the process of FIG. 11).

FIG. 13 is one embodiment of a flowchart illustrating an example of a method that may be performed to request additional information from third-party and/or from a user.

FIGS. 14-18 are example user interfaces that illustrate a user experience as the account discovery system accesses transaction data items of the user and attempts to identify accounts within the transaction data that can be added to the user's credit data.

FIG. 19-20 include embodiments of example user interfaces that may be presented to a user after scan of the consumer transaction data is completed and, in this example, accounts that may be added to the user's credit data are located.

FIGS. 21-22 are conceptual diagrams illustrating example transaction data items that may be identified in transaction data of the consumer and analyzed to determine whether the groups transaction data items are indicative of an account that can be added to credit data of a consumer.

FIG. 23 illustrates an embodiment of a user interface that may be provided to a user after an initial scan of transaction data items has been performed.

FIG. 24A is another embodiment of an example user interface that provides information regarding an identified account in transaction data items of user, with an option that is selectable by the user to add the account to credit data of the user (as a self-reported account).

FIG. 24B illustrates an embodiment of an example user interface that provides an overview of self-reported accounts that have been added to the credit data of the user.

FIG. 24C illustrates an embodiment of an example user interface that summarizes the various areas of consumer credit that may impact credit worthiness of the user.

FIG. 25 is an embodiment of a block diagram illustrating an account discovery system in communication with a financial institution, a user device, and a credit bureau.

FIG. 26 is an embodiment of a flowchart illustrating one embodiment of a method of providing a new trade line request to a credit bureau to initiate addition of a self-reported account to credit data of the user.

FIG. 27 illustrates an embodiment of example user interfaces associated with addition of a new account to credit data of the user.

FIG. 28A illustrates embodiments of example user interfaces that may be provided to a user to indicate availability of additional product offers, such as credit offers, in view of an increase credit score, such as may be caused by the addition of a new self-reported account to credit data of the user.

FIG. 28B illustrates an embodiment of an example user interface that may be provided after the consumer has boosted their credit file by adding one or more self-reported accounts.

FIG. 28C is an embodiment of an example user interface that may be provided to the user as part of an online credit report that is accessible to the user, either through a free or paid account with a credit reporting agency or other authorized credit reporting entity.

FIG. 28D is an embodiment of another example user interface that may be provided to the user as part of an online credit report.

FIG. 29 provides embodiments of example user interfaces that may be used in a trade line removal process.

FIG. 30 is an embodiment of a flowchart illustrating one embodiment of a method that may be performed to provide updated offers to a user responsive to an increase in credit score of the user that is caused by addition of one or more self-reported accounts to credit data of the user.

FIG. 31 is an embodiment of an example user interface that may be provided by and offer provider, such as an offer provider that prescreens users for credit card offers and provides information regarding matching credit cards to the user.

FIG. 32 includes embodiments of example user interfaces that may be displayed on a mobile device of a user to invite the user to engage the account discovery system to potentially increase the credit score of the user and potentially allow more offers to be provided to the user.

FIG. 33 is an embodiment of a flowchart illustrating one embodiment of a method that may be performed by the account discovery system to provide users with an estimated score increase that they may expect prior to adding new trade lines to their credit file.

FIG. 34 illustrates embodiments of example user interfaces that may be provided to users to indicate possible credit score changes.

FIG. 35 illustrates an embodiment of another example user interface that displays a similar estimate of credit score increase likelihood.

FIG. 36 illustrates an embodiment of an example user interface that may be provided to a consumer who wishes to stop periodic reporting of payment activity for one or more self-reported accounts.

FIG. 37 is an embodiment of an example user interface that may be provided to the user that wishes to dispute information associated with a self-reported account, such as an account that is added as a trade line to credit data of the user by the account discovery system discussed herein.

FIG. 38 is a block diagram illustrating one embodiment of an account discovery system that may be used to implement certain systems and methods discussed herein, such as providing a credit report to a user, gathering transaction data regarding non-traditional credit accounts of users, verifying account information with the user, adding the accounts as a self-reported accounts in the credit data of the user, and updating users' credit scores based on newly added self-reported accounts.

DETAILED DESCRIPTION OF EMBODIMENTS

Although several embodiments, examples and illustrations are disclosed below, the systems and methods described herein extends beyond the specifically disclosed embodiments, examples and illustrations and includes other uses of the embodiments and modifications and equivalents thereof. Embodiments are described with reference to the accompanying figures, wherein like numerals refer to like elements throughout. The terminology used in the description presented herein is not intended to be interpreted in any limited or restrictive manner simply because it is being used

in conjunction with a detailed description of certain specific embodiments. In addition, various embodiments can comprise several novel features and no single feature is solely responsible for its desirable attributes or is essential to practicing the embodiments herein described.

FIG. 1 is an embodiment of a flow diagram illustrating example components and example communications between the components of an embodiment of an authenticated access and aggregation database platform. In the example of FIG. 1, multiple data items 10, which may be accessed or received from one or more third-party entities, such as via a direct application programming interface (API) communication channel, are analyzed to determine whether any of the data items 10, or combinations of data items 10, meet rules for addition of the data items 10 to secure third-party risk item database 70. In general, the item database 70 stores and maintains database records for a plurality of users, each having one or more associated data items.

In this example, aggregation unit 20 accesses the multiple data items 10, and identifies groupings (also referred to as "subsets") of data items each associated with a common entity. For example, multiple data items of a user stored in a third-party database may be included in a grouping. A categorization unit 30 may then apply rules to the groupings of data items to identify groupings that match one or more patterns indicative of groupings of data items that should be added to the item database 70.

Authentication unit 40 allows a user of a user device 50 to provide authentication credentials that uniquely identify the user as associated with a set of data items in a particular data item database, such as a database operated by a particular third-party entity. In some embodiments, the authentication unit 40 also receives authentication credentials via the aggregation unit 20, for example. Thus, authentication of the user may occur at various levels. In some embodiments, the user is the owner of data items associated with the user and can control, set, change, and/or issue electronic permissions for use of varying sets, silos, individual data items, or even particular pieces of data within a data item, via the authentication unit 40.

The authentication unit 40 may then provide a set of authenticated data items 60 to item database 70, such as multiple data items 10 that were aggregated to a particular grouping of data items associated with the user, and matching a rule for addition to the items database 70. The user may then authenticate the grouping of data items, via input from the user device 50, to authenticate the grouping of data items for addition to the item database 70.

The item database 70, after receipt of authenticated data items 60, may determine that information of the corresponding database record, such as a record associated with the user, is to be updated. For example, the authenticated data items 60 may include a grouping of data items each associated with a particular entity (different than the entity from which the data items were accessed) that the user authenticated as begin associated with an account that the user would like to add to the item database 70, such as in a new database record associated with the user. Communication of the authenticated data items 60 to the item database 70 may occur via a secure communication channel established via an application programming interface (API).

In some embodiments, the item database 70 includes records associated with unique identifiers (for example, a key value and/or index value) for users. The system may determine that the received authenticated grouping of data items are associated with a particular database record because the authenticated data items include information

that associates them with the particular database record. For example, the authenticated data items may include the unique user identifier, and/or the authenticated data items may include another identifier that may be used to map to the unique user identifier by reference to additional information. The system may then determine that the authenticated data items include additional information regarding the user that is not already in the database record for the user, and may therefore update the database record with the new information.

In some instances, the system may determine that the corresponding database record is not to be updated. For example, the authenticated data items may include one or more groupings of data items that are already included in the database record of the user. Accordingly, no update may be necessary, or in some instances the database record or associated database items may be updated to indicate that a duplicate of the authenticated data items was received.

The system may generate a log of each database record update performed by the system. In some implementations, the log includes one or more (which may include all) data items included in the corresponding database record, including any newly added grouping of data items. Further, the log may include an indication of the change or update that was performed in the item database 70.

Database record updates/changes may be continuously logged as the item database 70 is updated. Logging updates to the item database 70 may speed up later evaluation of triggers. For example, as described below, triggers may be evaluated against the log of record changes, and may not need to be evaluated against the records database 70 as a whole. This aspect may significantly reduce processing power needed to generate event notifications. Further, because much information related to the updated record may be included in the log, the system may not need to re-query the database to generate notifications, further making the process of generating notification more efficient and less processor intensive. In some implementations, logs of database record updates may be stored in a historical database.

The triggers database 80 maintains rules indicating when alerts should be transmitted to entities responsive to changes in the item database 70. For example, the triggers database may maintain rules or criteria for transmitting a notification 90 to a user (such as via the user device 50) in response to certain changes in the database record of the user in the item database 70. For example, the user may establish such criteria based on various levels of granularity, so that the user is alerted of only those changes to their database record at the item database 70 of particular interest to the user. For example, a user may indicate that an alert should be sent to the user device 50 in response to addition of a new account data (associated with a grouping of data items) to the user's record in the item database 70. Thus, the trigger database 80 may monitor continuously or periodically, changes to the item database 70, apply trigger rules for each of a plurality of users, and transmit notifications accordingly.

The notification 90 may be in various forms, which may be selected by the user, by the system, and/or set as a system default. For example, notification 90 may be a push notification to a mobile application on the user device 50, which may cause an immediate display of the notification information on the user device screen, text message, email, and/or update to an online portal that the user may access to review additional information regarding the users database record with the item database.

In the example of FIG. 1, a notification 92 is also transmitted to third-party device 52. For example, a third-

party may establish rules that periodically identify user records within the item database 70 that each have a pre-determined set of characteristics. In this embodiment, the notification 92 may include a list of user information, and/or some or all of the corresponding user records from item database 70, that match the third-party established rules.

Aggregation unit 20 may aggregate account data from financial institutions, such as the data items 10. As an example, aggregation unit 20 may download transaction data items 10 associated with users from financial institutions, such that the users can review the transaction data from one or more financial institutions in one place. Aggregation unit 20 may also provide transaction data to the categorization unit 30, which is similar to the account discovery systems discussed below, such as after receiving authorization from users to provide such transaction data to the categorization unit.

Financial institutions may include, as examples, institutions maintaining demand deposit accounts (for example, checking and savings accounts) or other accounts (for example, credit card accounts, revolving card accounts, prepaid cash card accounts, reloadable card accounts, and so forth) on behalf of users, including accepting deposits into users' accounts and processing payments (including check and electronic payments) out of users' accounts to third parties such as utility or rent providers. Financial institutions may provide transaction data to account discovery system showing users' payments to utility and rent providers (for example, at the direction or authorization of said users).

Vendors or service providers may include various service providers such as landlords (for example, rental service providers), telecoms (for example, providers of telephone, internet, wireless accounts, cable, media such as television, movies, games, music, and other related services), and utilities (for example, providers of electricity, gas, water, trash, and related services). In general, service providers may include any entity which is regularly paid by users, such that those payments can be used as an indicator of credit risk associated with the user, and as discussed herein, added as a trade line in a users' credit data. For example, service provider accounts may include accounts for payment of child care, school tuition, gym memberships, after school programs, daycare service, medical care, home owners association dues, country club dues, insurance (such as, for example, automobile insurance, life insurance, medical insurance, dental insurance, vision insurance, disability insurance, and so forth), sports team dues, as well as other service provider account payments. While much of the disclosure references rental and utility providers, accounts with other service providers may also be added to users' credit data and used in credit scoring algorithms.

Terms

To facilitate an understanding of the systems and methods discussed herein, a number of terms are described below. The terms described below, as well as other terms used herein, should be construed to include the provided descriptions, the ordinary and customary meaning of the terms, and/or any other implied meaning for the respective terms. Thus, the descriptions below do not limit the meaning of these terms, but only provide example descriptions.

The terms user, individual, consumer, and customer generally refer to single persons, as well as groups of users, such as, for example, married couples, households, or domestic partners, organizations, groups, and business entities. Additionally, the terms may be used interchangeably. In some

embodiments, the terms refer to a computing device of a user rather than, or in addition to, an actual human operator of the computing device.

User Input (also referred to as Input) generally refers to any type of input provided by a user that is intended to be received and/or stored by one or more computing devices, to cause an update to data that is displayed, and/or to cause an update to the way that data is displayed. Non-limiting examples of such user input include keyboard inputs, mouse inputs, digital pen inputs, voice inputs, finger touch inputs (for example, via touch sensitive display), gesture inputs (for example, hand movements, finger movements, arm movements, movements of any other appendage, and/or body movements), and/or the like.

Credit data generally refers to user data that is collected and maintained by one or more credit bureaus (for example, Experian, TransUnion, and Equifax) and is subject to regulatory requirements that limit, for example, sharing of credit data to requesting entities based on the Fair Credit Reporting Act (FCRA) regulations in the United States and/or other similar federal regulations. Regulated data, as used herein, often refers to credit data as an example of such regulated data. However, regulated data may include other types of data, such as HIPPA regulated medical data. Credit data can describe each user data item associated with a user, for example, an account balance, or any combination of the user's data items. Credit file and credit report generally refer to a collection of credit data associated with a user, such as may be provided to the user, to a requesting entity that the user has authorized to access the user's credit data, or to a requesting entity that has a permissible purpose (for example, under the FCRA) to access the users credit data without the user's authorization.

Credit Event (also referred to as an event) generally refers to information associated with an event that is reported by a financial institution to one or more credit bureaus and/or the credit data system discussed herein. The credit events may include, for example, information associated with a payment, purchase, bill payment due date, bank transaction, credit inquiries, and/or any other event that may be reported to a credit bureau. Typically one credit event is associated with one single user. For example, a credit event may be a specific transaction, such as details regarding purchase of a particular product (for example, Target, \$12.53, grocery, and so forth) or a credit event may be information associated with a credit line (for example, Citi credit card, \$458 balance, \$29 minimum payment, \$1000 credit limit, and so forth, such as a periodic (for example, monthly) provision of summary information regarding the credit line of the consumer that is provided by the credit issuer.

Non-traditional Credit Data generally refers to data that is not generally included in FCRA regulated credit data of consumers, such as consumer data stored by one or more bureaus. Types of nontraditional credit data may change over time, such as if the FCRA revises regulations to allow or require credit bureaus to store additional types of consumer data as credit data. Depending on the jurisdiction, nontraditional credit data types may include rental, utility, and/or telecom data, for example.

Self-Reported Account generally refers to a consumer account with a vendor or service provider, such as a utility, telecom, or rental company, that is added to credit data of the consumer at the request of the user. The account discovery system discussed herein provides an example of a computing system that may interact with a user to identify and update credit data of the user to include accounts that are Self-Reported Accounts. In general, self-reported accounts

are associated with non-traditional credit data, such as utility, rental, and/or telecom payment data.

DDA Account generally refers to a checking, savings, or money market account of a user, but could be any other type of account. DDA accounts typically allow the user to deposit to and withdraw from the account substantially immediately, such as on demand, for example, through use of a credit card, debit card, paper check, online check, electronic transfer, and so forth.

While DDA accounts are discussed herein as sources for transaction data from which transactions of a user may be accessed, in some implementations additional types of accounts, such as credit card, PayPal, Venmo, and/or other currently existing or later developed payment platforms, may be used in identifying new consumer trade lines. Thus, any reference herein to a DDA account, or any specific type of DDA account, should be interpreted to include other embodiments where other types of accounts, such as credit card accounts, are accessed in place of (or in addition to) the referenced DDA account.

Financial institution generally refers to a bank or lender with which a user may have a DDA account, such as a bank with which a user may have a checking or savings account.

Trade line generally refers to credit data associated with a financial account of a user. For example, a checking account at a particular financial institution may be a first trade line of a user, while a savings account at the same, or another, financial institution may be a second trade line of a user. Trade lines may be summarized in credit data of users, such as by providing information regarding the financial institution, account balance, last account payment amount, payment status over prior months, and so forth.

Transaction and transaction data item generally refer to a particular payment from one entity to another entity. For example, a transaction may include Bob purchasing coffee on Friday morning. A transaction data item associated with that transaction may include data about the transaction, such as that it occurred on Aug. 10, 2018 and \$7.18 was paid to Coffee123 from Bob's checking account 123 at Bank XYZ. Transaction data items may indicate transactions using various user accounts, such as checking account, savings account, or credit card account. While discussions herein of transaction data items is primarily with reference to transaction identified in DDA account data of a user, transaction data items may also include transaction in a credit card account, or other credit-based account, of the user. Thus, the groupings and analysis of transaction data items that is discussed herein is not limited to only DDA account data, but also may include credit card transaction (and other payment account) data. As another example, cash, cashier check, money order, wire transfers, and other similar forms of payment may be included in transaction data items that are analyzed by the account discovery system. Such forms of payment may require additional validation procedures, such as a photograph of a receipt from the payee.

Application Programming Interface (API) generally refers to a defined communication channel, protocol, settings, and so forth that allows two devices to exchange information between one another in a more direct manner than might otherwise be possible. In some embodiments, an API registration module may be configured to register individual devices (for example, computing devices, Internet of things devices, sensors, and so forth) for communication with a particular computing device (for example, a central server that receives, processes, stores, provides, information to the individual devices) by issuing a security token (for example, such as an API token or an API key) to

the individual devices that authorizes such direct communications. Thus, a computing system may establish secure and direct communication channels with multiple devices via APIs.

Example Embodiments

The credit score is an important indicator of a user's financial health. A user's credit score may impact availability and/or terms (for example, interest rate) of such things as loan applications, rental applications, and real estate mortgages, as well as impacting the user's ability to find employment. Therefore, users have a substantial interest in monitoring and improving their credit scores.

Making timely payments and having those payments reported to national credit bureaus may improve a user's credit score. However, the types of financial accounts for which data is reported to the credit reporting agencies (CRAs), otherwise referred to as credit bureaus, is limited. For example, certain types of consumer accounts that could be used as indicators of risk associated with a lender extending credit to the consumer have not been historically included in credit data that is reported to the credit bureaus. In particular, telecommunications, utilities, real estate rentals, and other types of accounts associated with recurring statements, are not included in most credit score algorithms used by the credit bureaus. Thus, consumers that have good payment history with a home rental are not able to use that payment history in improving its the consumer's credit score. Accordingly, it may be desirable for a user to add telecommunications, utility, rental, and/or other recurring accounts (for example, records of payments to utility and rental providers) to users' credit data in order to improve the users' credit scores and related risk scores. Various systems and methods discussed herein provide a networking device architecture, as well as software usable on the various computing devices, to address this need for additional types of payment information being reportable to the credit bureaus. Other examples of recurring accounts that may be identified and added as trade lines to credit data of users may include accounts for payment of child care, school tuition, gym memberships, after school programs, daycare service, medical care, home owners association dues, country club dues, insurance (such as, for example, automobile insurance, life insurance, medical insurance, dental insurance, vision insurance, disability insurance, and so forth), sports team dues, as well as any other service provider account payments.

Some users, particularly those with poor credit scores or limited credit data, may benefit from adding non-traditional credit data to their credit reports. As an example, a user with limited credit data may see a significant boost in their credit score by adding, to their credit data, a utility account, showing recurring on-time payments to a utility provider, and a rental account, showing recurring on-time rent payments to a landlord. The present disclosure describes systems and methods that provide a technology platform for identifying and adding non-traditional credit data, such as rent and utility trade lines, to users' credit reports. Such accounts may then be referred to as self-reported accounts of the consumer. Additionally, the present disclosure describes issues that arise when attempting to add rent and utility accounts, such as issues with obtaining transaction data and assessing the reliability of transaction and account data.

FIG. 2A is an embodiment of a block diagram illustrating an account discovery system **110** (also referred to herein simply as the "system **110**") in communication with various external devices and systems via a network **160**. In this example, the system **110** is an indication with multiple

transaction providers **100** (generally including one or multiple transaction providers **100A**, **1008**, **100C**, or any other number of transaction providers). Transaction providers may financial institutions that provide DDA accounts to users, such as to consumers or businesses. As discussed further below, transaction providers store transaction data, in the form of transaction data items corresponding to individual transactions of the account holder, in secure databases that limit access to the consumer data. As described below, the account discovery system **110** advantageously provides a technical solution to allowing the system **110** to access transaction data of consumers have one or more transaction providers **100** using authorization credentials provided by the DDA account holder.

In the embodiment of FIG. 2A, the account discovery system **110** is also in communication with a user device **120** (which may refer to the user alone, the user computing device alone, or the combination of the user and the user computing device), a third-party system **130**, and a credit bureau **140**. The account discovery system **110** includes data permissioning component **112**, account identification component **114**, account verification component **116**, trade line update component **117**, and updated credit score usage component **118**. In some embodiments, these components are distributed amongst multiple computer systems, servers, devices, and so forth, and/or among different entities, such as with one or more third-party entity that performs some of the functionality discussed with reference to the component. In some embodiments, the transaction providers **100** facilitate transactions between the user device **120** and the third-party system **130**. For example, the transaction provider **100A** may be a first financial institution with which the user has a checking account. Thus, the transaction provider **100A** may facilitate payment of a monthly goods or services fee to the third-party system **130** via an electronic or printed check sent to the third-party system **130**.

In one embodiment, the data permissioning component **112** provides a communication channel with the transaction providers **100**, such as via application programming interfaces (API's) of the particular transaction providers. Thus, the data permissioning component **112** advantageously allows the account discovery system **110** to access transaction data items of the user. With access to the transaction data items of the user, the account discovery system **110** may analyze the transaction data items to potentially identify one or more recurring payment accounts that are not already included in the consumer's credit data. As an example, the data permissioning component **112** may store users' usernames and passwords or security tokens in order to download transaction data from the financial institutions. As another example, the data permissioning component **112** may store records, certificates, or other material enabling the user account discovery system to download transaction data directly from financial institutions or via account aggregation services.

In the embodiment of FIG. 2A, the account identification component **114** analyzes transaction data from one or more transaction provider **100** (for example, from one or more financial institutions) in search of sets of transaction data items indicative of a particular type of account, such as, for example, a recurring payment rental, utility, or telecom account. In some embodiments, the rules for identification of a particular type of account based on a set of transaction data items varies based on the particular type of account. For example, a rental account may have different identification criteria than a cellular telephone account. In some embodiments, the account identification component **114** may cal-

culate a confidence level indicating likelihood that an identified account (for example, an identified rental, utility, or telecom account) is actually an account of the identified type. For example, the confidence level may indicate likelihood that a set of transaction data items really are indicative of a rental account of the consumer, rather than related to other transactions (for example, monthly payments to an ailing relative).

In one embodiment, the account verification component **116** performs account verification, such as by interacting with the user and/or one or more third-party system **130** to verify that the appropriate account type has been associated with the set of transaction data items and/or that the account is truly associated with the particular user.

In one embodiment, the trade line update component **117** provides information to one or more credit bureaus requesting addition of an identified and verified user account (for example, a “self-reported account” of the user) to credit data of the user. For example, the trade line update component **117** may format and compile information regarding a new account to be added to credit data of the user in different formats for each of multiple different credit bureaus and generate a secure data packet storing such information to be transmitted to a remote system. Additionally, the trade line update component **117** may coordinate periodic updates to trade line data stored at the credit bureau **140**, such as monthly updates to a rental account that was added to the credit data of the user previously by the trade line update component **117**.

In one embodiment, the updated credit score usage component **118** provides updated credit information regarding the user (for example, an updated credit score of the user that considers a newly added rental account) to credit requesters. For example, a new account (or trade line in the credit data of the user) may be considered by various credit scoring algorithms in calculating risk scores of the user. Thus, if a new rental account of the consumer is added to the consumer’s credit data, and the consumer has a history of on time rental payments, the consumer’s credit score may increase immediately, or very soon, after addition of the new rental account information at the one or more credit bureaus. In some embodiments, the updated credit score usage component **118** provides alerts, such as in real time as credit data of a user is changed.

In some embodiments, the account discovery system **110** includes a user interface module (not shown) that interfaces with users. As an example, the user interface module may generate user-facing user interfaces, such as the user interfaces shown in the figures discussed below. Additionally, the user interface module may receive inputs and commands from the users, such as via interface with the user interfaces. As examples, the user interface module may receive a user’s agreement with terms and conditions, may receive a user’s identification of which financial institution to connect to, may receive credentials for connecting to an identified financial institution, may receive confirmations of and/or revisions to transaction data, may receive additional verification information such as copies of a lease agreement, and so forth.

FIG. 2B is one embodiment of a block diagram illustrating another example embodiment of an account discovery system in communication with various external computing systems and devices. In this embodiment, the account discovery system **110A** includes the account verification component **116** and the updated credit score usage component **118**. However, a separate account access system **202** includes the data permissioning component **112** and the

account identification component **114**. In one embodiment, the account access system **202** is operated and controlled by a third-party to the owner of the account discovery system **110A**. For example, the account access system **202** may have relationships or be configured to electronically communicate with multiple transaction providers **100**, such as the illustrated transaction provider **100A** in FIG. 2B that allow the account access system **202** to access transaction data of the user via user device **120**. The transaction providers **100** may be financial institutions, such as banks, lenders, creditors, and/or other facilitators of transactions. For example, the account access system **202** may communicate with the user device **120** to obtain credentials for accessing the user’s DDA account information at the transaction provider **100A** (such as a financial institution), and then make use of an API **204** to access DDA account information from the transaction provider **100A** immediately and/or periodically in the future. The DDA account information, for example, including multiple transaction data items, may then be analyzed by the account identification component **114** to identify potential accounts of the desired account type (for example, rental, utility, telecom, etc.). For example, the transaction provider **100A** may have previously provided payment(s) to one or more of the utility provider system **130A** (such as gas, electric, water, power, solar, or other utility provider), telecom provider system **130B** (such as mobile phone provider, phone service provider, internet service provider, cable or satellite television provider, or the like), or other provider **130C**, and so forth), and stores transaction data items for each of those payments. These transaction data items stored at the transaction provider **100A** may be accessed by the account access system **202** to identify self-reported accounts that may be added to credit data of the user. Information regarding the identified accounts may then be provided to the account discovery system **110A** to verify with the user and/or third-party (for example, the utility provider system **130A**, telecom provider system **130B**, or other provider **130C**) and to provide verified accounts to the credit bureau **140**.

In this way, the account access system **202** maintains a layer of security between the account discovery system and the consumer’s financial data held by the financial institution (or other transaction provider **100**). In other embodiments, the various components **112**, **114**, **116**, **117**, and **118** may be combined or separated, various computing systems and/or entities. For example, in one embodiment each of the components **112**, **114**, **116**, **117**, and **118** are operated by different entities.

FIG. 3 is one embodiment of an example user interface that may be provided to a user to initiate an account discovery process. In this particular example, the user interface **300** includes credit score information **310**, which includes a current credit score of the user in this example. The example user interface **300** also includes a potential score improvement interface **320**, which illustrates estimated likelihood of improvement in the consumer’s credit score in response to adding additional non-traditional trade lines to the consumer’s credit data. In this particular example, the estimated likelihood of improvement is based on improvements realized by a similar group of consumers, such as consumers that have reticular overlapping attributes as the current user. The example user interface **300** further includes information regarding account types that may be identified by the system and added to the credit data of the user to potentially improve the credit score of the user. In particular, the credit improvement interface **330** illustrates that an electric account, water account, and wireless account

could be added to the credit data of the user to potentially increase the user's credit score. In this example, the system has identified that these three account types are not currently in the crediting of the user and, thus, are good candidates for potentially improving the credit score of the user. Any of the user interfaces discussed herein may be provided in part or in whole by a server system (such as, for example, via a web browser access a secure web portal) or may be provided by an application that runs locally on the user device. Additional user interfaces, as well as systems and methods for providing features similar to those discussed herein, may be found in U.S. Provisional Applications No. 62/727,479, titled "System for authenticated access, aggregation, and categorization of database records," filed on Sep. 5, 2018, and No. 62/826,319, titled "Authenticated access and aggregation database platform," filed Mar. 29, 2019, each of which are hereby incorporated by reference in their entireties and for all purposes.

In one embodiment, the systems and methods discussed herein provide an authenticated access and aggregation database platform. For example, in one embodiment a data processing system is disclosed for data processing, including database and file management, as well accessing one or more databases or other data structures, authenticating users, and categorizing data items for addition to the database system. In some embodiments, the system may be configured to coordinate access to user account information via user-provided authentication credentials; apply account identification rules to the accessed account information to identify a plurality of accounts of the user; and initiate updates to a database record associated with the user indicative of any accounts identified.

In one embodiment, a computerized method of obtaining information regarding user accounts is performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system to perform operations comprising receiving, from a user computing device, a request to access financial account information associated with a user, selection of a financial institution indicator from a plurality of financial institution indicators indicated in a user interface on the user computing device. The method may further include receiving, from an account access system, account data associated with a financial account of the user with a payee, the account data indicating an account type and an associated payee, wherein the financial account is a rental account, a utility account, or a telecommunication account. The method may further include receiving, from the user computing device, confirmation that identified account type for the payee is accurate, a request to add the financial account with the payee to credit data of the user. The method may further include generating, based on portions of the plurality of transaction data items and the account data associated with the payee, a trade line creation data package, the trade line creation data package formatted for ingestion by a credit bureau to initiate addition of the trade line to credit data of the user, transmitting the trade line creation data package to the credit bureau, requesting a credit score of the user from the credit bureau, wherein a credit scoring algorithm executed by the credit bureau to generate the credit score is based at least partly on portions of the plurality of transaction data items or the account data included in the credit data of the user. The method may further include providing credit score change information to the user computing device.

In one embodiment, the method may further include receiving, from the user computing device credentials for accessing financial account information associated with the user at the selected financial institution, the credentials including a username and a password, selection of a financial account of the user at the financial institution via the user interface on the user computing device, the user interface displaying one or more of a checking account, a savings account, or a credit card account of the user at the financial institution. The method may further include accessing a plurality of transaction data items of the selected financial account of the user at the financial institution. The method may further include selecting a first transaction data item of the plurality of transaction data items, determining a payee identified in the first transaction data item, identifying a subset of transaction data items each indicating the determined payee, wherein the subset of transaction data items includes at least the first transaction data item and one or more other transactions data items. The method may further include, for individual payees, determining, based at least on the identified subset of transaction data items, account data associated with a financial account of the user with the payee, the account data comprising at least one or more of a number of payments, an annual payment amount, average payment amount, or average number of days between payments. The method may further include applying a first account identification rule, associated with a first account type, to the account data, the first account identification rule based on one or more of the number of payments, the annual payment amount, the average payment amount, or the average number of days between payments, determine, based on said application of the first account identification rule, a first confidence level indicating likelihood that the financial account is the first type of account. The method may further include applying a second account identification rule, associated with a second account type, to the account data, the second account identification rule based on one or more of the number of payments, the annual payment amount, the average payment amount, or the average number of days between payments, determine, based on said application of the second account identification rule, a second confidence level indicating likelihood that the financial account is the second type of account. The method may further include, if the first confidence level is higher than the second confidence level, identifying the financial account as of the first type of account, if the first confidence level is lower than the second confidence level, identifying the financial account as of the second type of account.

In one embodiment, the systems and methods discussed herein provide user permissions for access to secure data at third-party. For example, in one embodiment a user permission system manages and regulates access to secure data at one or more third-party data sites. The system may provide access to one or more databases or other data structures based on user authentication and access rules that have been established, such as by a user associated with the data being accessed at the third party data store. Access may be provided via an API to the third-party data site, along with access credentials of a user with data stored with the third-party data site, allowing the system to access data on behalf of the user.

In one embodiment, a computerized method of obtaining information regarding user accounts is performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system to perform operations comprising

transmitting user interface data to a user computing device, the user interface data configured to depict a permissions interface element that is selectable to indicate authorization to access financial account information associated with the user, receiving, from the user computing device, authorization to access financial account information associated with the user. The method may further include, in response to receiving the authorization to access financial account information associated with the user, receiving, from the user computing device, selection of a financial institution from a plurality of financial institutions indicated in a user interface on the user computing device, receiving credentials for accessing financial account information associated with the user at the selected financial institution, identifying an API key associated with the selected financial institution, transmitting, to an online address of a system in electronic communication with the selected financial institution, the API token and the credentials, receiving, via the system, indicators of one or more financial accounts of the user with the selected financial institution, receiving, from the user computing device, selection of a financial account of the one or more financial accounts, accessing, via a secure communication session initiated with the API token, a plurality of transaction data items of the selected financial account of the user at the financial institution. The method may further include transmitting user interface data to the user computing device, the user interface data configured to depict a user interface on a display of the user computing device, the user interface including one or more interactive elements selectable to indicate authorized uses of the transaction data items by the computing system, receiving, from the user computing device, selection of authorized uses of the transaction data items, selectively sharing, based on the authorized uses of the transaction data items, the transaction data items with one or more third parties.

In some embodiments, the authorized uses of the transaction data items include one or more of use in: identifying recurring payments, updating credit data of the user, calculating derived attributes, or calculating a risk score. In some embodiments, transaction data items associated with a post date more than one year prior to a current date are disregarded. In some embodiments, transaction data items associated with a post date more than two years prior to a current date are disregarded. In some embodiments, the access component is operated by the computing system. In some embodiments, the access component is operated by a third-party.

In one embodiment, a computerized method performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system to perform the computerized method comprises accessing a plurality of data items associated with a user via an application programming interface (API) communication channel established with a third-party database, selecting a first data item of the plurality of data items, determining a recipient identifier in the first data item, accessing a recipient data structure storing indications of associations between recipient identifiers and corresponding recipients, wherein a first recipient is associated with a plurality of recipient identifiers used by different third-party databases to identify the first recipient, determining that the recipient identifier is associated with the first recipient in the recipient data structure, scanning the plurality of data items to identify a subset of the data items each associated with the recipient identifier, wherein the subset of data items includes at least the first data item and one or more other data items,

determining, based at least on the identified subset of data items, account data associated with an account of the user with the first recipient, the account data comprising at least one or more of a number of data items each having time stamps within a predetermined time period; or an average number of days between time stamps of sequential data items, applying a first account identification rule, associated with a first account type, to the account data, determining, based on said application of the first account identification rule, a first confidence level indicating likelihood that the account is the first type of account. The method may further include, in response to determining that the first confidence level exceeds a threshold confidence level, initiating addition of the account to the secured third-party risk database.

In one embodiment, a computerized method of identifying accounts of a user each associated with a plurality of transaction data items is performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system to perform the computerized method comprising accessing a plurality of transaction data items indicative of transactions of a user with one or more financial institution, selecting a first transaction data item of the plurality of transaction data items, determining a payee identifier in the first transaction data item, accessing a payee data structure storing indications of associations between payee identifiers and corresponding payees, wherein a first payee is associated with a plurality of payee identifiers used by different financial institutions to identify the first payee, determining that the payee identifier is associated with the first payee in the payee data structure, scanning the plurality of transaction data items to identify a subset of the transaction data items each associated with the payee identifier, wherein the subset of transaction data items includes at least the first transaction data item and one or more other transactions data items, determining, based at least on the identified subset of transaction data items, account data associated with a financial account of the user with the payee, the account data comprising at least one or more of: a number of payments, an annual payment amount, an average payment amount, or an average number of days between payments, applying a first account identification rule, associated with a first account type, to one or more of the number of payments, the annual payment amount, the average payment amount, or the average number of days between payments of the account data, determining, based on said application of the first account identification rule, a first confidence level indicating likelihood that the financial account is the first type of account, in response to the first confidence level exceeding a threshold confidence level, determining an expected risk score impact of including the account data a risk data set associated with the user, in response to the expected risk score exceeding a threshold, initiating addition of the account data to the risk data set associated with the user.

The method may further include selecting, based on the account data, the first account type from a plurality of account types including at least a rental account type, a utility account type, and a telecommunication account type. The method may further include selecting, based on the account data, the first account type from a plurality of account types that each require recurring payments from account holders. The method may further include applying a second account identification rule, associated with a second account type, to the account data, the second account identification rule based on one or more of the number of

payments, the annual payment amount, the average payment amount, or the average number of days between payments, and determining, based on said application of the second account identification rule, a second confidence level indicating likelihood that the financial account is the second type of account. In one embodiment, the plurality of transaction data items are indicative of transactions of the user with a first financial institution and a second financial institution, a second transaction data item from the second financial institution includes a second payee indicator that is different from the first payee indicator, and the first payee indicator and the second payee indicator are each associated the first payee in the payee data structure.

In one embodiment, the systems and methods discussed herein provide generation of data structures based on categories of matched data. For example, in one embodiment a data processing system communicates with a secure third-party database to provide updated user data that is then usable by a plurality of other entities. In some embodiments, the system may be configured to coordinate access to user account information via user-provided authentication credentials, apply account identification rules to the accessed account information to identify a plurality of accounts of the user, and initiate updates to a database record of the user at the secure third-party database associated indicative of any accounts identified.

In one embodiment, a computerized method of updating user risk data, the computerized method performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system to perform the computerized method comprises receiving, from a user computing device, a request to update credit data of the user with account information regarding an account identified in direct deposit account data of a financial payment account of the user, generating a trade line creation data package including an identifier of an issuer of the account identified in the direct deposit account data, a data furnisher identifier associated with an entity that provides consumer data to a credit bureau; and at least a portion of the account information formatted for ingestion by a credit bureau to initiate addition of the account to credit data of the user. The method may include identifying an API key associated with the credit bureau, and transmitting the API key and the trade line creation data package to the credit bureau, wherein the account information is usable by the credit bureau to update a risk score of the user.

The method may further include periodically receiving payment information associated with the account from the direct deposit account data of the financial payment account; and transmitting the periodically received payment information to the credit bureau.

The method may further include executing a credit scoring algorithm to generate the credit score of the user based at least on the account information stored by the credit bureau.

In one embodiment, the systems and methods discussed herein provide a database platform for realtime updating of user data from third party sources. For example, in one embodiment a data processing system communicates with a secure third-party database to obtain information about a user that is usable to determine one or more items associated with the user. The system then coordinates gathering and identification of additional data relevant to the user from other third-party data sources, to potentially update the user's information stored with the secure third-party data-

base. The updated information may then be accessed at the secure third-party database to determine items associated with the user, which may include additional items in view of the additional data.

In one embodiment, a computerized method, performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system to perform the computerized method comprises determining identification information of a user, obtaining a current risk score associated with the user, determining a first one or more product offers available to the user based on the current risk score, determining a second one or more product offers not available to the user based on the current risk score, determining an estimated risk score of the user based on hypothetical addition a new trade line of the user to risk data of the user, in response to determining that at least one of the second one or more product offers would be available to the user based on the estimated risk score, providing an option to the user to initiate updates to risk data of user, in response to the user selecting the option to initiate updates to risk data, initiating communication of the user with an account discovery system, receiving, from the account discovery system, an indication of an updated risk score of the user, wherein the updated risk score is higher than the current risk score based on addition of the new trade line to risk data of the user by the account discovery system, determining at least one of the second one or more product offers that are now available to the user based on the updated risk score, and providing the at least one of the second one or more product offers to the user. The method may include providing credit score change information to the user computing device.

In one embodiment, the systems and methods discussed herein are usable in estimating changes to user risk indicators based on modeling of similarly categorized users. For example, in one embodiment a data processing system communicates with a secure third-party database to obtain information about a plurality of users and generates a model usable to identify other users with similar characteristics. A scoring algorithm may be selected for use on user data based on the associated users identified with the model. The scoring algorithm determines an estimated score change for the user, and may provide the user information regarding how the user can achieve the estimated score change.

In one embodiment, a computerized method, performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage device storing software instructions executable by the computing system to perform the computerized method comprises accessing a score impact rule indicating one or more account types that impacts credit scores of users, accessing credit data of a user, identifying a plurality of accounts included in the credit data, determining account types of the plurality of accounts in the credit data, identifying a first account type of the one or more account types that impacts credit scores of users that is not included in the determined account types of the plurality of accounts of the user, execute a score impact algorithm, based at least on the first account type and credit data of the user, to determine a possible credit score change if an account of the first account type is added to the credit data of the user. The method may include providing, to the user, an indication of the possible credit score change.

The method may include identifying a plurality of other users associated with addition of accounts of the first account type, analyzing account data of the plurality of other

users, based on the aggregated account data, generating the score impact algorithm configured to determine, for respective users, possible credit score changes based on addition of accounts of the first account type.

In some embodiments, other users are identified as users having accounts of the first account type with account attributes within predetermined threshold of the account attributes of the account of the user.

In some embodiments, the predetermined threshold is of payment history, payment amount, or account subtype of the accounts.

Example System and Process

FIG. 4 is one embodiment of a block diagram illustrating various components and processes that may be performed according to various embodiments discussed herein. Depending on the embodiment, certain implementations may include fewer or additional blocks than illustrated in FIG. 4, and/or the blocks may be performed in an order different than illustrated. Additionally, while the blocks are illustrated in functional groups, each of these functional groups may be performed by multiple computing systems and/or entities, and conversely, multiple functional groups may be combined for performance by a single computing system and/or entity.

The illustration of FIG. 4 includes functional modules for data permissioning, account identification, account verification, trade line updating, and updated credit score usage. However, the functional modules could be partitioned differently in certain embodiments. In the example of FIG. 4, the functional blocks 462, 464, 466, 467, and 468 are generally associated with components 112, 114, 116, 117, and 118, respectively. In other embodiments, functionality in a particular block of FIG. 4 may be divided among different components and/or functionality in multiple blocks of FIG. 4 may be combined into a single component.

Beginning with block 402, the user engages an account discovery system, such as a system that may be controlled and/or operated by a credit bureau. Account discovery systems may include credit bureaus, such as Experian, TransUnion, and Equifax, as well as agents of credit bureaus, such as entities that provide credit data to users that is accessed from one or more credit bureaus, but is made available to the user via a third-party user interface (for example, via a website or mobile application). In some embodiments, the user provides login credentials, or establishes a credit monitoring account with a credit bureau, in order to access credit information via the account discovery system 110.

In some embodiments, the user accepts terms and conditions 404 agreeing to the account discovery system's rights and responsibilities, authorizing performance of the functional modules of FIG. 4, and agreeing to the accessing, storing, maintaining, sharing, and so forth, of the user's personal information, such as information that may be obtained from financial institutions doing business with the user. In some embodiments, the user has previously accepted terms and conditions 404 that include authorization for performance of the remaining functional modules of FIG. 4.

Data Permission

In the embodiment of FIG. 4, a data permission module 462 performs functions that allow the user to select a financial institution 410, provide credentials for the financial institution 412, and select a direct deposit account (DDA) or other account at the financial institution 414 from which transaction data of the user should be accessed. In one

embodiment, the functions of the data permissioning module 462 are performed by the data permissioning component 112.

At block 410, the user may be provided with a user interface that lists, or allows the user to search for, a financial institution (or other transaction provider 100) with which the user has a DDA account. In other embodiments, the user may indicate a financial institution in other manners. Next, in block 412, the user provides credentials that allow the account discovery system 110 (FIG. 1), the account access system 202 (FIG. 2), or another system, to access the user's financial information held with the selected financial institution. For example, a user with a checking account with XYZ bank may select XYZ bank at block 410 and then at block 412 provide a login and password that is usable to access the user's XYZ bank transactional data via XYZbank.com, or via an application programming interface (API) that communicates with XYZ bank. In some embodiments, transactional data includes a plurality of transaction data items that each correspond with a transaction between a payee (or other entity) and a user (for example, a consumer looking to identify accounts for addition to the consumer's credit file). Depending on the embodiment, the credentials provided at block 412 may be secured through use of a third-party account access and/or aggregation service, such as the account access system 202, so that the user is not required to provide their financial institution credentials (for example, their login and password for that financial institution) to the account discovery system 110. In such embodiments, the user may authorize the account discovery system 102 to access DDA account data via the third-party service, which may itself have access to the user's records at the financial institution.

Moving to block 414, the user selects a particular DDA account held at the financial institution, such as from a list of DDA accounts that is retrieved directly from the financial institution by the data permissioning component 112 (whether performed by account discovery system 102 or another system/entity). For example, the user may be provided with an option to select one or both of a XYZ bank checking account or a XYZ savings account after providing credentials for XYZ bank in block 412. In some embodiments, the user may be allowed to connect a credit card account also, so that transaction data items include payments made through the credit card account. While FIG. 4 references a DDA account at a financial institution, other accounts with other entities may be used in various implementations.

Depending on the embodiment, user authentication may be performed using various methods and based on various information. For example, authentication information may comprise a user-selected personal identifier, a username/password combination, biometric data (for example, faces, fingerprints or eye scans), and/or other information that can be used to authenticate a user. Similarly, various authentication protocols may be implemented to authenticate the user and/or any entities that are requesting information regarding the user's credit information, such as the service providers discussed herein. For example, a requesting user may send an electronic request to a token gateway environment (of the account discovery system 110 or account access system 202) with credentials, and then the token gateway environment may validate the credentials with a security and access management environment using a standard open protocol such as OAuth (for example, OAuth 2.0, which is generally an authorization framework that enables applications to obtain limited access to user accounts).

Account Identification

In the example of FIG. 4, an account identification component 464, at block 420, identifies accounts based on transaction data items within the selected DDA account (for example, the account selected in block 414) that may be added as trade lines to a user's credit data. In one embodiment, the account identification component 114 (for example, FIGS. 1 and 2) identifies accounts by finding patterns of transactions that indicate a high likelihood those transactions are associated with an account that can be added as a trade line to a user's credit data. In some embodiments, the account identification component (or other component) also determines whether an account that can be added to the user's credit data should be added to the user's credit data. For example, transaction data items associated with an electrical utility account (for example, Southern California Edison) of a user may meet criteria for adding the account to credit data of the user (for example, the monthly payment amounts, timing of the payments, payee information, and so forth, indicate that the transaction data items are for an electrical utility), in some situations addition of the account as a trade line to the user's credit data actually decreases the credit score of the user, for example, if the user paid less than the full amount due each month. Thus, rules or criteria for identifying accounts could include those identifying accounts that are likely qualified for addition to the user's credit data and further identify which of those accounts would have a positive impact on the credit score (and/or long term credibility of the user).

As another example of an account identification process that may be performed by the account identification module, transaction data items in Bob's checking account with XYZ bank may indicate that Bob has paid a regular amount to AI's Landlord Service on the last day of each month over the last two years. Thus, the account identification module may identify these regular transactions as being part of a rental account that may qualify for inclusion as a trade line in Bob's credit data (at one or more credit bureaus). Other types of accounts that may be identified include utility accounts (electrical, gas, water, and so forth), mobile phone accounts, and other accounts that are associated with payments indicative of credit worthiness of the account holder.

In some embodiments, the transaction processing of block 420 may be performed by the account discovery system 110, while in other embodiments a third-party that accesses and/or aggregates financial account information, such as account access system 202 (for example, as illustrated in FIG. 2B) may perform the transaction processing. In some embodiments, transaction data items from multiple accounts of the user, such as from both a checking account and a savings account of Bob (which may be at a common financial institution or at different financial institutions), are analyzed to identify potential accounts for addition as trade lines to the user's credit file. Thus, in such an embodiment, even if Bob alternates his monthly rental payments between his different accounts (even accounts at different financial institutions), the account identification component 114 may associate the payments with a common rental account. In some embodiments, transaction data items (or, more generally data items) may be accessed from other data sources, such as non-financial data sources. For example, data items indicating rental payments may be obtained from the landlord (or rental/leasing company) for analysis in identifying data items indicative of a rental account of the user and/or for verifying a rental account of the user.

In some embodiments, the account identification component 114 applies or executes one or more models that are

configured to categorize transactions across multiple months or years of transactional data of the user. For example, in some embodiments, the account identification component 114 may search transaction data items of a user for transactions that occur with a certain periodicity, within a certain monetary range of one another, with certain keywords or characters in the payee's name (or other information, such as a memo or "for:" information field provided by the user), and/or any other attributes that may be associated with transaction data for the user. Data item groupings may then be created to indicate sets of data items that are believed to be associated with a particular account of the user. In some embodiments, each data item groupings is associated with a different payee.

In some embodiments the account identification component 114 may calculate a confidence level or score indicating likelihoods that the particular transaction data item should be included in a grouping of data items. Thus, for a particular transaction data item (for example, \$4.58 purchase at Starbucks #417325 on Mar. 21, 2018 at 6:38 AM), multiple confidence levels may be calculated to indicate strength of correlation with multiple transaction groupings. In this implementation, the transaction data items may be associated with a transaction grouping for with a highest confidence level for the transaction data item was calculated. In some embodiments, a transaction data item confidence level may additionally need to exceed a threshold confidence level for the transaction data item to be associated with a grouping.

The account identification component 114 may associate an account type with each identified account (for example, each grouping of data items for particular payees) in the user's transactional data. For example, a first identified account (for example, associated with 24 separate monthly payments identified in Bob's checking account data) may be indicated as a rental type account. Account types may include a general account type (for example, telecom, utility) and/or a specific account type, or may have additional levels of categorization. For example, telecom account types may be further categorized as mobile phone, phone, internet, cable, or satellite accounts, while utilities account types may be further categorized as gas, electric, water, power, solar, or trash account.

In some embodiments, characteristics of transaction data items that are analyzed to help identify potential accounts of a given user may include payee identifier (or normalized payee identifier), description or memo associated with the transactions, transaction amount, transaction periodicity, and/or other related transaction characteristics. For example, in one embodiment information regarding the payee on each transaction (for example, in the transaction data item for the transaction) is normalized for matching with other transactions, such as from the same payee. For example, extraneous characters in the payee information, such as characters that are associated with a payment account or number of the transactions (for example, an electronic check number), may be removed or disregarded. Additionally, payee information may be standardized, such as by identifying a standardized identifier for a particular payee that may be associated with various adaptations of payee information for that particular payee. For example, a standardized identifier for a payee (for example, "Southern California Edison") may be associated with multiple variations of payee information that could be used by different financial institutions in identifying transactions with that payee (for example, "SCE", "So Calif Edison", and so forth). Thus, through standardizing payee information of transaction data items, matching of transac-

tion, even from multiple DDA accounts of the user, may be associated as payments to a particular account.

In some embodiments, additional data of a transaction data item may be normalized, standardized, or otherwise cleansed for use in matching the corresponding transaction with other related transactions (for example, other transactions to the same payee). For example, the description or memo associated with transactions may be analyzed and used in matching. For example, memo information that is handwritten on a paper check may be recognized using optical character recognition to determine the memo. A handwritten “rent” in the memo of rental payment checks each month may be used by the account identification component **114** to match the monthly rental payment checks as each being related to a rental payment of the user. Further, text input into a memo field may be parsed to be used in the matching. Additionally, in some embodiments the transaction amount of transactions is used in matching to other related transactions. For example, transactions of an identical amount (for example, to transactions for exactly \$29.99) may have a higher likelihood of each being grouped together as associated with a common payee and user account than transactions of different amounts. In some embodiments, a range or percentage variation in payment amounts may be determined as within a tolerance zone such that transaction data items that vary within the tolerance zone (for example, payment amounts within 5% of the average payment amount for the grouping) are not disqualified from being in the grouping associated with a particular payee. For example, an electrical account may vary from month to month depending on usage by the user that month. Thus, a transaction amount rule may indicate that transaction amounts within a range of 20% of an average transaction amount for a group of transactions does not disqualify the transaction as being associated with the electrical account of the user. In some embodiments, third-party data may be access to determine and/or adjust tolerance zones for grouping transaction data items with one another. For example, for an electrical account, whether information may be accessed for the month corresponding to a particular transaction data item to determine an expected change in electrical power usage based on weather conditions that might cause additional (or less) power use.

In some embodiments, the account identification component **464** identifies a transaction periodicity for transactions that are preliminarily identified as being associated with a common payee. For example, the account identification component **464** may calculate an average time between payments to Electric Company as 31 days, with the shortest time between payments as 26 days and the longest time between payments as 34 days. Other statistical values associated with timing of the transaction data items, such as median, mean, standard deviation, and so forth, may also be calculated in certain embodiments. This transaction periodicity may then be used as a factor in determining whether the transactions should be grouped as being associated with a common payee and, thus, with a particular account of the user.

In some embodiments, the account identification component **114** determines one or more confidence levels or scores for each identified grouping of transaction data items. For example, a confidence score may indicate a likelihood that the identified grouping of transaction data items is associated with an account of the indicated type. For example, the confidence level may be based on factors such as periodicity of transactions, amount of transactions, payee information, and so forth that may indicate likelihood that each of the

associated transactions are properly correlated with a particular payee and account of the indicated type. Thus, a lower confidence score may indicate that the identified transactions are only somewhat likely to be associated with a particular account type or trade line of the user, while higher confidence scores would indicate that the identified transactions are more likely associated with a particular trade line of the user.

Depending on the implementation, the account identification component **114** may determine an overall confidence level or score (for example, a single common score that indicates the overall likelihood that a grouping of transaction data items are associated with a particular type of account and/or with a particular payee) and/or may determine transaction-level confidence scores (for example, a score for each individual transaction, or for groups of transactions, each of which indicates the likelihood that that particular transaction, or group of transactions, is associated with a particular grouping of transaction data items and/or with a particular payee). In some embodiments, the confidence levels or scores may further consider a minimum frequency and/or recency requirement for addition of a self-report account as a tradeline in the user’s credit data. For example, some or all types of self-reported accounts may be required to have at least three payments within six months to even be considered for addition as a trade line. Thus, for an account with three payments within seven months, even if there is a high confidence level in the account type being appropriate for addition as a trade line (for example, the transaction data items are associated with a wireless account), the account will not be transmitted to the credit bureau for addition as a tradeline. In some embodiments, the frequency and recency requirements for addition of trade lines may vary based on account type.

In some embodiments, the account identification component (and/or the account verification component) validate ownership of a DDA account by the user to ensure that the appropriate user is provided the potential credit score boost from payments included in the DDA account. For example, an account ownership validation component may receive information regarding an account, such as name, address, email address, phone number, etc, from the financial institution. This account ownership information may then be compared to user information associated with the user’s account with the account identification system, such as a credit monitoring account. The account ownership information could be provided by the account access system, such as via an API communication to the account discovery system, so that the account discovery system may perform the account ownership validation matching and validation. Such account ownership validation may increase the likelihood that a user only gets credit for the accounts that they pay (and belong to them).

Account Verification

The account verification module generally processes the account information provided by the account identification component **464**, attempts to verify the account information as being accurate, and/or determines if additional information may be needed to confirm accuracy of the account information. For example, an account of a user should not be added to the user’s credit data unless the account accurately indicates payment activity of the user and, correspondingly, can be used as a factor in determining creditworthiness of the user. In the discussion below, an “account” is generally associated with a single payee (for example, a particular electric company, cellular provider, and so forth) as well as a grouping of transaction data items that have each been

determined to be associated with the single payee by the account identification component **464**. The accounts identified by the account identification component **464** may not include an account number provided by the payee since the account was identified based on transaction data items of the user that may not include the account number. As discussed below, in some embodiments additional information regarding an account, which may include an account number that is verifiable with the payee, for example, may be automatically collected and/or provided to the account discovery system.

At block **430**, a list of accounts for possible inclusion in credit data of the user is provided to the account verification module (whether provided by the same or different entity as the account identification component **464**). For example, the list of accounts may include, for each account, an account type, transactions associated with the account (for example, the transaction data items that were each categorized as associated with the account), a confidence score or scores, and/or other related information.

At block **432**, the user confirms accuracy of each of the identified accounts, or indicates that one or more of the accounts is not accurately reflected (for example, transactions indicated as associated with a cell phone account may not actually be associated with a cell phone account). In some embodiments, a user interface indicating the identified accounts, or potentially just those identified accounts having confidence scores below a threshold or minimum confidence score for positive identification of the account type, may be provided to the user. The user may then select, or deselect, identified accounts to indicate those that are accurate. In some embodiments, transaction data associated with an indicated account may be displayed for review by the user. Additionally, the user may indicate that an identified account is legitimate, but that one or more of the particular associated transactions are not associated with the identified account. For example, an identified utility account may be associated with 14 transaction data items (for example, payments) over the prior 12 month period, and the user may indicate that two of the indicated transactions are not associated with that particular utility account. In such embodiments, the account verification module (and/or other modules discussed herein) may update the transaction data items associated with the identified account, which may in turn update the confidence level that the account is of the determine type (for example, a utility type).

In some embodiments, the user can indicate missing transaction data items to be added to an account. For example, if a cellular service provider account is missing three monthly payments over a 12 month period, the user may indicate that the payments were made during those three months with information regarding the payments. For example, the user may indicate that the payments were made from another DDA account with another financial institution and provide credentials allowing the account discovery system to access transaction data items of the user at that other financial institution. The transaction data items may then be identified in the other DDA account data and combined with the grouping for the cellular service provider.

Moving to block **434**, for those accounts that the user has verified (for example, indicated are actual accounts of the user of the identified type at block **432**), a determination is made as to whether additional information may be needed from the user and/or a third-party before providing the account to one or more credit bureaus for addition as a trade line to the user's credit. Thus, in some embodiments one or more criteria or rules may be applied to the identified

account information to determine whether the account is sufficiently accurate and reliable for inclusion in the user's credit data. For example, a rule may indicate that for any identified rental accounts, additional account verification information is required before providing the new rental account to a credit bureau. As another example, a rule may indicate that a minimum number of transactions and/or minimum number of payments must be associated with an account for the account to qualify for addition to the user's credit data. In some embodiments, such a rule may vary based on the identified account type (and/or subtype), such that for a first account type (for example, rental) a minimum of eight payments are required, while for a second account type (for example, electricity), a minimum of 12 payments are required.

If additional information is needed (for example, the result of block **434** is a determination that additional information is needed), the process moves to block **436**, where additional information is requested from the user and/or a third-party. For example, a user may be asked to provide additional information, such as a typical monthly payment amount and/or payment date for a particular identified account. This additional information may then be provided back to the account identification module (and block **420** repeated) to better categorize transactions that may be associated with the account. For example, with the typical payment amount and payment date provided by the user, the account identification module may identify additional payments that were not initially identified (and, similarly, may exclude certain payments that were initially identified). Thus, the additional information may increase likelihood of the identified accounts being eligible for addition to the user's credit data. In some embodiments, the user may provide information regarding an account that was not identified in the initial account identification block **420**, so that the account identification module may potentially identify a new account only after the user provides additional information.

In some embodiments, a third-party is contacted for further information to verify a (potential) account of the user. For example, a mobile phone account may be verified with a request to the mobile carrier identified in the transaction data for the account. Such verification may be performed via an API call to the mobile carrier, which may return simply a binary (for example, yes or no) verification indication, or detailed transaction information regarding the account (such as payment history, payment timing, bill due dates, and so forth).

In some embodiments, the user and/or a third-party may provide documentation confirming authenticity of the identified account. For example, for an identified (potential) rental account of a user, the user may be asked to upload a scanned or photographed copy of a lease agreement that may be analyzed to confirm the rental account. In this example, the lease agreement may be automatically parsed (for example, after optical character recognition) and information, such as monthly payment amount, payment due date, landlord, and so forth, may be extracted and compared to account information included with that particular account (such as the grouping of transaction data items associated with the payee from the account identification module **464**).

In some embodiments, other information and/or data sources may be accessed to verify accuracy of financial accounts. In some embodiments, one or more of the processes of scanning the user's DDA account (block **420**), transmitting identified accounts (block **430**), providing the user an opportunity to confirm accuracy (block **432**), deter-

mining if additional information is needed (block 434) and requesting such additional information (block 436), may be repeated multiple times to enhance the accuracy of the identified account information and/or confidence level in categorization of transaction data. Additionally, in some embodiments the data permissioning process (beginning at block 410) may be performed as part of the account verification process to access additional transaction data items of the user from additional DDA accounts.

Trade Line Updating

In the embodiment of FIG. 4, if an account is verified by the user, and no additional information is needed (block 434), the account is provided to one or more credit bureaus for addition to the user's credit data. In some embodiments, at block 440, the user is provided an opportunity to decide whether or not the account is added to the user's credit data. In some embodiments, an estimate of impact on the user's credit score may be provided to the user, such as an expected credit score increase (or decrease) before the user decides whether or not to add the account as a trade line to the user's credit data. Depending on the embodiment, this expected (or "simulated") credit score may be generated using the same scoring model or algorithm as is used to provide the user with their actual credit score (for example, that would appear in the user's credit report). In some embodiments, the expected credit score, or credit score change (for example, a plus or minus amount), may be determined based on a different model or algorithm, such as a scoring algorithm that is developed by the account discovery system 102 based on previous changes in credit scores of other users due to addition of particular types of accounts and/or accounts with particular ranges of attributes (for example, payment history, payment amount, account subtype, and so forth). Thus, in some embodiments, a scoring model may be developed and improved over time, such as by a machine learning algorithm that analyzes credit information of users before and after addition of new trade lines for patterns in how credit scores are affected by such additions of trade lines. In some embodiments, such a scoring model may also consider user demographics and credit history in developing an algorithm for predicting credit score impact by the addition of new trade lines. For example, a user with a thin credit file (for example, less than two trade lines) may benefit greatly by addition of a cellular service account, while a user with a thick credit file (for example, eight or more trade lines) may not see a credit score impact by addition of the same cellular service account. In some embodiments, the system generates an improvement metric that is reflective of other users that match one or more characteristics of the user. In some embodiments, an estimated credit score is not provided to the user prior to adding the account to the user's credit data (for example, a newly generated credit score may only be provided after the new account is added as a trade line at block 440).

If the user indicates a desire not to add the account to the user's credit data at block 440, the process may end, or may return to a prior block, such as block 410 where the user is asked to connect to one or more additional financial institutions, to block 430 where a list of accounts already identified is provided to the user, or to another block.

At block 442, the account discovery system updates profile information of the user to indicate the added trade line. In some embodiments, the account discovery system may generate or estimate the user's credit score based on account information (for example, trade line information) maintained by the account discovery system (or by a credit bureau or other entity that controls the account discovery

system), such as without requesting credit data from a credit bureau. Additionally, the user profile information may be provided to the user in various formats and levels of detail, such as in user interfaces that are displayed to the user via a mobile application, web browser, text messages, and so forth, and which allow the user to interact with the provided information.

If the user requests the addition of the account to credit data of the user (at block 440), at block 444 the account discovery system generates a new trade line request for transmission to a credit bureau (or multiple credit bureaus in some embodiments). For example, the account information may be formatted in the same manner as account information provided by a typical credit data furnisher, such as a credit card lender that regularly provides account information to credit bureaus for addition (or updating) of trade lines associated with its credit card holders. In some embodiments, the format is the Metro 2 format. In other embodiments, other formatting may be used to prepare account information for transmission to the credit bureau. In some embodiments, the format of the trade line request is customized for the particular credit bureau. For example, a first format may be used for transmission to the first credit bureau while a second format is used for transmission to a second credit bureau. In some embodiments, communication with credit bureaus may be accomplished via API calls.

At block 446, the credit bureau receives the formatted trade line information (generated at block 444) and processes the information to add the trade line to the user's credit data. In some embodiments, the credit bureau applies the same requirements for adding new trade line information to a user's credit file as would be applied to other trade line information (for example, from other data furnishers). Thus, if the trade line information is not usable to uniquely identify a user in the credit bureau's data, the trade line information may not be added to the requesting user's credit data or, depending on the circumstances, may be added with reference to a newly added credit record for the user indicated in the trade line information.

In some instances where trade line information is transmitted to the credit bureau, a trade line for the payee may already exist in the user's credit data. Thus, the transmitted trade line information may be used to supplement the account information (for example, to include additional transactions that are not already reflected in the user's credit file).

Updated Credit Score Usage

In the embodiment of FIG. 4, with the user's credit data updated with the newly added trade line, the user's credit score may be impacted. For example, the user's credit score may increase, and such increase may make the user eligible for financial or other products for which the user was not eligible minutes before with the lower credit score.

At block 450, one or more scoring models may be applied to the user's credit data (including the newly added trade line) to generate updated credit scores for the user. For example, a scoring algorithm that includes utility account data as an input variable may be evaluated after addition of a utility trade line to the user's credit data to produce an updated (for example, higher) credit score for the user.

Various entities may apply scoring algorithms and/or otherwise access credit data of users. For example, in some embodiments the credit bureau may apply a credit scoring algorithm periodically to each users' credit data, such as nightly, so a credit score that is no more than 24 hours old is always quickly available to requesters. In some embodiments, the credit bureau may apply a credit scoring algo-

rithm in response to requests for credit data of a particular user, such as in real-time in response to receiving an inquiry for credit data of a user. In some embodiments, the credit bureau may apply a scoring algorithm provided by another user risk assessment entity, such as by providing credit data of the user to a scoring server configured to analyze the credit data using a proprietary credit scoring algorithm and output to the credit bureau the resultant credit score for the user. Thus, in some embodiments, the account discovery system **110** may not know how particular credit data of users' impacts credit scores generated using the proprietary credit scoring algorithm. In other embodiments, other entities, such as financial institutions, marketing companies, and so forth, may generate risk scores based on credit data, and possibly other data, of the user.

At block **452**, the updated credit score of the user may be used in identifying offers to provide to the user. For example, the account discovery system **110** may receive an indication of the user's new credit score (after addition of a new rental, utility, or telecom trade line, for example) and determine whether the user is prequalified for one or more financial products, such as credit cards, personal loans, refinance loans, car loans, and so forth. Such financial products may not have been available to the user or may only have been available on less desirable terms (such as a higher interest rate) prior to addition of the new rental, utility, or telecom trade line to the user's credit data (for example, Alice's credit score may have increased from 600 to 625 after adding a rental trade line indicating she has regularly paid her rent over a two-year period, and Bank XYZ Bronze Credit Card may only be offered to users with a credit score above 620). Depending on the embodiment, the updated credit score (and/or additional user credit data) may be compared to offer criteria by the account discovery system **102** and/or another entity, such as directly by a financial institution.

At block **454**, the user receives a notification of a change in credit data, such as an indication that the user's credit score has changed. The notification of block **454** may be one example of notification **90** sent to user device **50** of FIG. **1**. In some embodiments, the notification is provided to the user via the user interface through which the user initially engaged the account discovery system **102**, for example, within seconds of the user requesting that a newly identified and verified account be added to the user's credit file. In other embodiments, an alert or notification may be provided to the user in other manners, such as a SMS message delivered to a telephone number associated with the user (for example, a telephone number stored in the credit bureau's data of the user or in the user profile stored by the account discovery system **102**) or a push notification to a mobile application, such as a credit management application provided by the account discovery system **102**. In any case, the alert may advantageously be delivered to the user's mobile (and/or other) device in substantially real-time to when the change to the user's credit file occurred so that the user can immediately make use of the updated credit score (for example, by applying for a new credit line) or, if the change to the user's credit file is not correct or even fraudulent (for example, added by someone other than the user), the user can take action to dispute the updated credit information as soon as possible. In some embodiments, a software module monitors credit bureau data for changes to credit data of users, or changes to credit data that impacts a credit score of the user in some embodiments, and initiates delivery of an alert to the user as the change is detected. For example, when a new rental trade line is added to a user's credit data, such

a module may detect addition of the trade line and initiate an alert to the user. Such alerts may be transmitted directly from the credit bureau or via another entity, such as the account discovery system **102**. In some embodiments, the user alert (block **452**) is transmitted in response to detection of a change to the user's credit data that has been transmitted from the credit bureau, such as when an updated credit score of the user is received at the account discovery system **102**. Depending on the embodiment, alerts may be associated with rules that specify which types of changes to the user's credit data should be provided in real-time alerts.

In some embodiments, the account discovery system **102** requests an updated credit score of the user after providing the new trade line information to the credit bureau. Account discovery system **102** may request the updated credit score immediately after providing the new trade line information or after some amount of elapsed time (for example, one second, five seconds, and so forth after transmitting the trade line data to the credit bureau). Thus, in this embodiment the account discovery system **102** may receive the newly calculated credit score of the user within seconds of addition of the trade line to the user's credit file. After the new calculated credit score is received, the account discovery system **102** may optionally display to the user a change in the user's credit score (for example, a plus or minus amount) attributable to the newly added account.

In some embodiment, after the user has been shown an updated credit score, an option to remove a trade line from the user's credit file is provided via the user interface. For example, if the user adds a new utility account to the user's credit data, such as via the method discussed above, a newly calculated credit score may be displayed to the user via the account discovery system website, mobile application, text message, and so forth. If the newly calculated score is lower than a previous score of the user, for example, the new utility account trade line actually decreased the user's credit score, the user interface may provide an option for the user to remove the new trade line credit data. For example, a button, check-box, link, or other user interface feature associated with removal of an account from credit data may be selected by the user to initiate a removal process. In response to a request for removal of a trade line, the account discovery system **102** may transmit a properly formatted request to one or more credit bureaus requesting removal of the trade line.

In various embodiments discussed herein, alerts and/or notifications (which may be used interchangeably) are automatically transmitted to a device operated by the user whose credit data has been updated and/or requested (for example, such as notification **90** sent to user device **50** of FIG. **1**). The alert and/or notification can be transmitted at the time that the alert and/or notification is generated or at some determined time after generation of the alert and/or notification. When received by the user's device, the alert and/or notification can cause the device to display the alert and/or notification via the activation of an application on the device (for example, a browser, a mobile application, and so forth). For example, receipt of the alert and/or notification may automatically activate an application on the device, such as a messaging application (for example, SMS or MMS messaging application), a standalone application (for example, a credit monitoring application provided to the user by the credit report access control system), or a browser, for example, and display information included in the alert and/or notification. If the device is offline when the alert and/or notification is transmitted, the application may be automatically activated when the device is online such that the alert and/or notification is displayed. As another

example, receipt of the alert and/or notification may cause a browser to open and be redirected to a login page generated by the system so that the user can log in to the system and view the alert and/or notification. Alternatively, the alert and/or notification may include a URL of a webpage (or other online information) associated with the alert and/or notification, such that when the device (for example, a mobile device) receives the alert, a browser (or other application) is automatically activated and the URL included in the alert and/or notification is accessed via the Internet. The alert and/or notification may be determined based on preferences stored in a data store. For example, a user may sign up for a publish/subscribe service or a credit monitoring service that may be configured to identify changes to credit data. After enrollment, the individual may additionally select an option to be notified of credit data inquiries and a selection of preferences for receiving alerts/notifications.

Calculation of Expected Score Boost

In some embodiments, an estimate of impact on the user's credit score may be provided to the user, such as an expected credit score increase (or decrease) even before the user provides permission to the account discovery system to identify new trade line's (for example, at block 402). For example, an expected credit score impact may be calculated for users based on an expected impact of adding an account type (for example, an electrical account) that is currently missing from the user's credit data, and perhaps that is typically included in credit data, to the user's credit data. The account discovery system and/or an affiliated system may provide the expected credit score increase associated with the addition of an electrical account to the user as an incentive for the user to engage the account discovery system.

Depending on the embodiment, this expected (or "simulated") credit score may be generated using the same scoring model or algorithm as is used to provide the user with their actual credit score (for example, that would appear in the user's credit report). In some embodiments, the expected credit score, or credit score change (for example, a plus or minus amount), may be determined based on a different model or algorithm, such as a scoring algorithm that is developed by the account discovery system 102 based on previous changes in credit scores of other users due to addition of particular types of accounts and/or accounts with particular ranges of attributes (for example, payment history, payment amount, account subtype, and so forth).

In one implementation, a score impact rule indicating one or more account types that impact risk scores of users are accessed. Next, an API key associated with the financial institution is identified and transmitted to the financial institution with a request for transaction data of the user. Via secure communication channel established with the financial institution, transaction data items of the user are obtained. Next, a plurality of groupings of the accessed data items are identified, such as groupings of data items associated with an entity. An account type for each of the groupings of data items may be determined, and then a first account type that impacts credit scores of users that is not included in the determined account types of the user may be identified. This account type represents a type of account that could be added to the credit data of the user to potentially impact credit score of the user. A score impact algorithm may be executed to determine a possible risk score change if an account of the first account type is added to the risk data of the user. The score impact algorithm may be based on the first account type and the existing credit data of the user.

Thus, in some embodiments a scoring model may be developed and improved over time, such as by a machine learning algorithm that analyzes credit information of users before and after addition of new trade lines for patterns in how credit scores are affected by such additions of trade lines. In some embodiments, such a scoring model may also consider user demographics and credit history in developing an algorithm for predicting credit score impact by the addition of new trade lines. For example, a user with a thin credit file (for example, less than two trade lines) may benefit greatly by addition of a cellular service account, while a user with a thick credit file (for example, three or more trade lines) may not see a credit score impact by addition of the same cellular service account. In some embodiments, an estimated credit score is not provided to the user prior to adding the account to the user's credit data (for example, a newly generated credit score may only be provided after the new account is added as a trade line at block 440).

Example Methods

FIG. 5 is an embodiment of a flowchart illustrating one example of a process of interacting with a consumer, accessing DDA account data of the consumer, identifying non-traditional account(s) of the consumer in the DDA account data, and updating credit data of the consumer at a credit bureau. In one embodiment, the method of FIG. 5 is performed by the account discovery system. Depending on the embodiment, the method of FIG. 5 may include fewer or additional blocks and the blocks may be performed in an order that is different than illustrated.

Beginning at block 510, an account discovery system may be accessed by a user. For example, the user may visit a website of a credit monitoring service, such as may be provided by a credit bureau. The user may contact the account discovery system in response to an advertisement or other communication offering to help the user increase the user's credit score and/or qualify for a financial account. The user may then provide the account discovery system authorization to access DDA transaction data of the user at one or more identified financial institutions. As an example, the account discovery system may receive a user's authorization together with the user's username and password for a particular financial institution, such that the user account discovery system can prove to the financial institution it is authorized to retrieve the user's transaction data. In some embodiments, other forms of authentication of the user are requested for decreasing likelihood that a fraudster is attempting to access the user's financial account data. Further details of receiving the user's authorization to access DDA transaction data are discussed below.

Moving to block 520, the account discovery system accesses DDA transactions at the identified financial institution(s). Block 520 may involve downloading records of some or all of the DDA transactions made available to the user by the identified financial institution(s). In some embodiments, the access to DDA transactions is via an API communication channel that is established between the account discovery system and the financial institution. In other embodiments, the DDA transactions are accessed via a front end interface, such as the same or similar user interface that may be displayed to the user.

Continuing to block 530, the account discovery system categorizes the DDA transactions. For example, the user account discovery system identifies, from a plurality of transaction data items accessed at the indicated financial institution, a group of transactions associated with a particular payee. As an example, the system may identify

monthly recurring transactions made to the same payee as being categorized together and associated with a single account (for example, an electric, water, or wireless account). Additionally, the system may identify a second set of transaction data items made to another payee and, based on account identification rules, determines that the second set of transaction data items are associated with a rental account of the user.

At block **540**, the account discovery system receives a user's confirmation of the identified accounts. For example, the user account discovery system may identify, in block **530**, a particular set of transaction data items as being associated with a particular utility account, may identify that the utility account is believed to be of a certain type (such as an electricity bill from a given utility), and may identify various attributes of the account such as the average payment, the maximum payment, the minimum payment, and so forth. Then, in block **540**, the user account discovery system may provide at least some of this identified information to the user and receive the user's verification that the information is correct. The user may verify that individual transactions are properly categorized, that the identified account is correctly identified, and so forth.

At block **550**, the user account discovery system may assess the reliability of the identified account and may, optionally, obtain additional information to verify that the account is of the type indicated. For example, the user may be asked to take a driver license photo, use an app to scan in a document (for example, associated with the account), provide electronic authorization to request automatic sending of electronic verification from a third-party (such as the account issuer), and so forth. Further details of account verification processes are discussed below.

At block **560**, the account discovery system initiates addition of the account(s) as trade line(s) in the user's credit data. For example, the system may generate a data package formatted for ingestion by a particular credit bureau to allow the credit bureau to add the account as a new trade line of the user.

At block **570**, the account discovery system recalculates the credit score of the user, based on the newly updated credit data (for example, including any newly added trade lines).

At block **580**, the user account discovery system provides the updated credit score to the user and/or to third-parties. The updated credit score can be used by such third parties in determining whether to offer credit, and at what terms to offer said credit, to the user. By including additional trade lines such as rent and utility accounts, the updated credit score may more accurately reflect the credit worthiness of the user. In some embodiments, the updated credit score may be provided to, and usable, by the user and/or authorized third parties substantially immediately after the account is added as a new trade line to credit data of the user. For example, the credit score of the user may be recalculated in substantially real-time in response to addition of a new trade line to credit data of the user, and the recalculated credit score may similarly be provided to the user and/or authorized third parties substantially real-time in response to calculation of the updated credit score.

Example System, Method, and User Interfaces for Accessing DDA Data of Users

FIG. 6 is an embodiment of a block diagram illustrating another example of an account access system **202** and an account discovery system **110A** in communication with one another (whether operated by a single and the or by separate entities). In this embodiment, three transaction providers

100 A, **100 B**, and **100C** are in communication with the account access system **202** via respective APIs **204A**, **204B**, and **204C**. Thus, in this embodiment, data permissioning process, such as performed by the data permissioning component **112**, may be performed via communications with transaction providers **100** that is initiated and authenticated using API tokens, keys, and/or other similar secure communication credentials. For example, the transaction provider **100 a** may be a first financial institution that allows direct access to transactions of its customers (for example, consumers with DDA accounts at the financial institution) via a secure communication channel that is initiated through use of an API token that has been issued to the account access system **202** by the financial institution. In this way, the transaction provider **100 a** maintain security of consumer information by limiting access to the consumer DDA account information to only those with a pre-issued API token. Similarly, communications with transaction providers **100 B** and **100 C** may be performed with unique API keys or tokens issues from those transaction providers. In some embodiments, the transaction providers may include, or may use third-party, API token service, which interfaces with external entities (for example, the data permissioning component **112**), receives authorizations from the external entities indicating that the account access system **202** has sufficient rights to access transaction data items of consumers held by the transaction provider, and issues a API token to the account access system **202** usable to initiate a "back-end" communication channel with the transaction provider to efficiently and quickly access data to which the account access system **202** is authorized. Thus, in some embodiments the account access system **202** provides the API token issued to the account access system **202** in conjunction with a request for transaction data items of a particular consumer.

The data permissioning component **112** may further communicate with the user device **120** to obtain credentials that allow the data permissioning component **112** to access transaction data items of the user at a transaction provider. These user credentials may include a login ID and password for a particular transaction provider, or any other credentials that the user may have been issued that allow the user and/or the account access system **202** to access transaction data items in the user's secure account with the transaction provider. The data permissioning component **112**, with a valid API token issued from a transaction provider and access credentials from the user device **124** that transaction provider, may initiate communication with the particular transaction provider and access transaction data items of the user with that transaction provider.

In the embodiment of FIG. 6, the account access system **202**, which includes the data permissioning component **112** and the account identification component **114**, may be operated and/or controlled by an entity separate from the account discovery system **110A**. For example, the account discovery system **110A** may be operated by a credit reporting agency, while the account access system **202** is operated by a financial account aggregator. Through separation of the functionality performed by these two entities, consumer privacy of information may be maintained. For example, in some embodiments the account access system **202** accesses individual transaction data items of the consumer at the one or more transaction providers **100**. However, those individual transaction data items may not be shared with the account discovery system **110A** (for example, a credit bureau). Rather, the account access system **202** may analyze the transaction data items to identify accounts that may be added to the consumer's credit data and provide only the

minimum information needed to the account discovery system **110A** for addition of the new account to credit data of the consumer. In other embodiments, the account discovery system **110A** receives and stores the transaction data items.

FIG. **7** is one embodiment of a flowchart illustrating one example of a method that may be performed to authorize and initiate access to a user's DDA account information at a financial institution. For purposes of illustration, the method of FIG. **7** will be discussed in conjunction with several example user interfaces in FIGS. **8-10**. In some embodiments, the method may be performed by the data permissioning component **112**, such as may be controlled by an account access system **202** (for example, FIG. **2B**). In other embodiments, the data permissioning component **112** may be operated by the account discovery system **110A** (for example, FIG. **2A**). Depending on the embodiment, the process of FIG. **7** may include fewer or additional blocks and or the blocks may be performed in order different than is illustrated.

Beginning at block **710**, a user provides authorization to the data permissioning component **112** to access DDA account information of the user at one or more transaction providers. For example, a consumer may authorize a credit bureau to initiate communication with a financial institution at which the consumer has a checking account for purposes of analyzing transactions in that checking account. For example, user interface **810** illustrates an example user interface that may be presented to a consumer on a mobile device, such as a cell phone or tablet. A similar user interface may be provided on a desktop computing device of a user or any other consumer electronic device. Any references herein to a mobile device or mobile user interface are provided for illustration purposes and should not be construed to limit implementations of the systems and methods herein to only those specifically mentioned mobile device or mobile user interfaces. Conversely, any mobile device or mobile user interface could also be implemented with a desktop, laptop, or other computing device and associated user interfaces.

FIG. **8** illustrates embodiments of three example user interfaces that may be displayed on a user device. User interface **810** illustrates security measures associated with the proposed access to the user's financial account data. The user can select button **822** to continue on to the data permissioning process. User interface **820** illustrates an introductory screen from an example credit reporting agency, "MyBureau", which could represent any credit bureau. Additionally, similar user interfaces may be provided by other entities, such as an aggregation entity. In the example user interface **820**, information regarding an example "Score Boost" process is provided to the user and the user is asked to select an interface element, such as button **812**, to initiate the process. In this example, after the user selects button **812**, a user interface **830** may then be displayed to the user, which request information from the user on a financial institution at which the user maintains a DDA account, such as a checking account, savings account, money market account, or the like. The example user interface **830** provides a listing of several "popular options," which may be stored as a predetermined listing based on one or more factors such as geographic location, and also allows the user to search for financial institutions that may not be listed already.

Returning to FIG. **7**, at block **720** a selection of a financial institution from the user is received, with reference to user interface **830** of FIG. **8**, the user may select one of the popular options of financial institutions or search for another

financial institution. After the user selects a financial institution at block **720**, credentials for accessing the user's financial information at the selected financial institution are received at block **730**. For example, a username and password that allow access to the users checking account information at the selected financial institution may be provided to the data permissioning component **112**. In an embodiment where the data permissioning component **112** is operated by a third-party entity (different than the account discovery system **110 A**, such as in FIG. **2B**), communication with the user may be directly between the data permissioning component **112** (for example, of the account access system **202** of FIG. **2B**) and the user device **120**. In this way, credentials to the users financial account at the financial institution are only disclosed to the account access system **202** and not also to the account discovery system **110 A**, providing increased security to the user by limiting dissemination of the user's login credentials. In some embodiments, the communication with the user device **120** is provided via a pass-through functionality (for example, using an iFrame or similar functionality) of the account discovery system **110 A**, such that the user is unaware that they are communicating directly with the account access system **202** (or other entity that provides the data permissioning component **112**) and the communication with the user are seamless as they proceed through the blocks of FIG. **7**. In such an embodiment, the user may be unaware that a separate data permissioning component **112**, possibly operated by a third-party to the account discovery system **110A**, is coordinating communication with the selected financial institution. In some embodiments, the user is alerted to the shift in communication from the account discovery system **110A** to the account access system **202** (or other entity it provides the data permissioning component **112**).

In one example implementation, the account discovery system may create a user record in an API from the account access system **202** (or more particularly, with the data permissioning component **112**). The account discovery system **110 A** may then generate a redirect URL and iFrame URL that are delivered to the user device (for example, user interface **910**). The user within interacts with the iFrame URL, such as to provide login credentials and two factor authentication information, directly with the data permissioning component **112**. After the user is authenticated with the financial institution, the account identification component **114** and/or other components of the account discovery system **110 A** may access financial account information of the user has the financial institution via an API connection established by the data permissioning component **112**. In one embodiment, after authorization to access a particular user's financial account information at a particular financial institution has been established, the data permissioning component **112** (and/or other related components) may request financial account information (for example, transaction data items) of the using a user-specific token, such as may be issued by the data permissioning component **112** and/or an API token generator/manager of the financial institution. Thus, the account identification component **114**, for example, may immediately and/or periodically in the future, access transaction data items of the user at the financial institution using an API call that includes the user specific token. In some embodiments, an entity token may also be required, such as a token issued to the data permissioning component **112** that authorizes the account access system **202** to access user data at the financial institution (for example, with a user specific token).

FIG. 9 illustrates embodiments of example user interfaces that may be provided by the data permissioning component 112, whether operated by a third-party account access system 202 or the account discovery system 110A, to obtain access credentials from the user. In other embodiments, other user interfaces, such as requesting other credential information from a user and/or providing different two-step authentication procedures, may alternatively be used. Example user interface 910 displays the name of the selected financial institution, “MyBank” in this example, with a request for the user to provide a User Name and Password for the MyBank account. After the user provides that information, user interface 920 initiates a two-step authentication procedure using a cell phone number associated with the user’s account at the selected financial institution. The telephone numbers associated with the user account may be provided by the selected financial institution, for example, MyBank, after the username and password have been accepted. An example of FIG. 9, the user is able to select one of multiple telephone numbers associated with the user’s financial account with a request that a security code be transmitted to the selected number. After one of the telephone numbers is selected by the user in interface 920, a security code is transmitted to the selected telephone number and user interface 930 is displayed, requesting entry of the security code received at the selected telephone number by the user. If the user cannot provide the security code, access to the users financial information at the financial institution is not allowed and, additionally, the user may be provided with a fraud risk alert. If the two-step authentication is completed successfully by the user providing the transmitted security code, access to the financial account of the user is allowed. In other embodiments, additional forms of two-step authentication procedures, such as use of an Authenticator application, and/or other authentication procedures may be implemented.

Next, at block 730, with the user authenticated at the financial institution (via the data permissioning component 112), the account identification component 114 and/or other components of the account discovery system 110A, may access the users financial account information. In the example of FIG. 7, at block 740 the user is presented with a list of accounts at the financial institution (for example, associated with the login credentials provided by the user), and an option to select one or more of the accounts. User interface 1010 in FIG. 10 illustrates an example user interface that may be presented to the user indicating multiple accounts identified at the financial institution, and providing the user an option to select one or more of the accounts from which the account access system 202 will be authorized to access specific transaction data items. In the example of user interface 1010, a checking account (for example, “MyChecking” with a balance of \$523) and a savings account (for example, “MySavings” with a balance of \$3,101) were identified in the user’s account data at the financial institution (for example, “MyBank”). In this example, the user selects the checking account, indicating that transaction data items in the user’s checking account may be accessed by the account discovery system. In this example, because the user did not also select the MySavings account, the users savings account information will not be made available to the account discovery system. User interface 1020 confirms that the user has granted access to “1 account” of the user with MyBank.

At block 745, a security token, such as an API token or key, is associated with the user account at the financial institution, so that the account identification component 114

and/or account access system 202 can use the security token to securely access transaction data items of the user at the financial institution. In one embodiment, a security token is an encrypted way of storing a username and password. It ensures that when the account discovery system is connecting to the financial institution of the user to get account information, it is safe and secure. For example, the security token may be provided to an API interface of the financial institution to authorize access to financial account data of the user at the financial institution. The security token may have a limited life (for example, two hours, two days, two weeks, and so forth) and may be associated with additional restrictions on use of the security token.

Moving to block 750, the account identification component 114 may use the established communication channel with the financial institution to access transaction data items of the user. For example, the account access system 202 may provide the user specific token (for example, as discussed above with reference to block 745) to the financial institution to obtain access to transaction data items in the one or more DDA accounts of the user associated with the user specific token (which the user previously authorized the account access system 202 to access).

At block 780, transaction data items of the user are accessed via a secure communication session with the financial institution. In some embodiments, transaction data items are copied to the account access system 202 for further analysis. In some embodiments, a subset of transaction data items, such as those within a predetermined time or meeting other filter criteria, are provided to the account access system 202.

At block 790, the transaction data items are accessible to the account identification component 114, for example, to analyze for indications of financial accounts (for example, utility, rental, telecom, and so forth) that may not already be in the credit data of the user, and which could be added to credit data of the user to potentially increase the credit score of the user.

Example System, Method, and User Interfaces for Categorizing Data Items

FIG. 11 is an embodiment of a flowchart illustrating one example of a method that may be performed to categorize data items (for example, transaction data items) from the transaction provider (for example, a financial institution). In some embodiments, the transactions data items are categorized or grouped according to a payee or recipient of a transaction. For example, multiple monthly payment transactions from a checking account to Power Company 123 may all be grouped as payments that are likely associated with an ongoing account of the user with Power Company 123. In other embodiments, data items may be categorized in groups in other manners. For example, transactions with multiple payees or recipients may be grouped, such as those that are each associated with a particular type of account. For example, multiple wireless provider accounts may be grouped together via a process similar to FIG. 11. For purposes of illustration, the method of FIG. 11 will be discussed in conjunction with several example user interfaces in FIGS. 14-15 and 18, as well as conceptual diagrams in FIGS. 16-17 of data items that may be grouped and account identification rules that may be applied to such grouped data items.

In some embodiments, the method of FIG. 11 may be performed by the data permission account identification component 114, such as may be controlled by an account access system 202 (for example, FIG. 2B). In other embodiments, the account identification component 114 may be

operated by the account discovery system **110A** (for example, FIG. **2A**). Depending on the embodiment, the process of FIG. **11** may include fewer or additional blocks and or the blocks may be performed in order different than is illustrated.

Beginning at block **1110**, a payee included in the transaction data items is selected. A user transaction data items, even with a single financial institution, may include dozens, hundreds, thousands or more transaction data items. Thus, categorization or grouping of the transaction data items may be initiated in various manners. For purposes of illustration, at block **1110**, a particular transaction data items included in the set of access transaction data items is selected for analysis. In some embodiments, multiple transaction data items may be concurrently selected and analyzed, such as via a process similar to that illustrated in FIG. **11**.

For the selected transaction data items, at block **1120** a payee identified in the transaction data item is determined. For some transaction data items, the payee is included in a separate payee field as digital information, for example, a payee may be indicated as "ABC Rentals" in a "PAYEE" field of a transaction data item. For some transaction data items, the payee may not be as easily identifiable. For example, a paper check may include a handwritten payee. The account identification component **114** may analyze the handwritten payee information, such as by using a handwriting analysis algorithm and/or other optical character recognition algorithm, to identify digital characters included in the payee field. For the example payee ABC Rentals, character recognition of a handwritten version of ABC Rentals may result in something that is not precise such as "ABC Reatils". Thus, correlation of transaction data items by payee may be technically challenging in such circumstances. In some embodiments, categorization of transaction data items associated with a recurring account of the user may be based on other parameters of the transaction data items, rather than or in addition to the payee identifier.

In some embodiments, the account identification component **114** performs a normalization and/or standardization process on data values of the transaction data items. For example, standardization may include removal of certain special characters (for example, symbols), correction of typographical errors (for example, which could catch the typo "Reatils" and correct to "Rentals") and/or perform other standardization processes. A normalization process may involve accessing a payee data structure associating a normalized payee identifier with one or multiple possible payee identifiers that could be located in transaction data items. Example, the payee data structure could include a standard payee identifier of "ABC Rentals" that is associated with multiple variations of that payee identifier, such as "ABC Rental", "ABC-Rentals", "ABC Rentals Inc.", and so forth. In this way, the account identification component **114** can more accurately associate transaction data items that are each involve a common payee.

In some embodiments, other data values of transaction data items are normalized, standardized, and used in generating groupings of similar transaction data items. For example, information provided in a memorandum or other informational field of a transaction data item may be analyzed.

After performance of block **1120** on a selected payee (block **1110**), a grouping of transaction data items, each associated with the selected payee, are identified. Thus, if the transaction data items are associated with monthly payments to the selected payee, and two years of transaction

data items are processed, the grouping of transaction data items identified at block **1120** may include 24 transaction data items.

Moving to blocks **1130-1150**, information summarizing, characterizing, or aggregating information in the grouping of transaction data items located at block **1120**, is performed. The information derived in blocks **1130-1150** is provided as examples of information that may be determined to help evaluate whether the grouping of transaction data items indicate an account of the user that potentially could be added to the credit data of the user. In other embodiments, other information may be derived from the grouping of transaction data items.

At block **1130**, an annual payment amount for the transaction data items is calculated. For example, transaction amounts for each transaction data item dated within a prior 12 month period may be summed to determine the annual payment amount. A similar process may be performed for a prior yearly period, such as transaction data items dated from 24 months prior to 12 months prior. Similarly, total payment amounts for other time periods may be developed, such as quarterly or semiannually.

At block **1140**, an average payment amount is determined. For example, an average payment amount over the prior one year period may be determined by averaging payments received over the last 12 month period.

At block **1150**, periodicity of payments is determined. For example, an average number of days between payments over the prior one year period may be determined by averaging the number of days between each pair of sequential transaction data items.

At block **1160**, the account identification component **114** determines whether there are additional payees in the transaction data items that have not yet been analyzed for categorization. In some embodiments, those transaction data items grouped with the transaction data item selected at block **1110** are not the selected for grouping. In other embodiments, each transaction data item, whether already associated with a grouping of transaction data items or not, is analyze with the method of blocks **1110-1150**. If additional payees have not yet been analyzed for categorization, the method returns to block **1110** where another payee is selected. If no additional payees need categorization, the method continues to process for identifying the type of account each grouping of transaction data items is most associated with and identifying any accounts that may be added to credit data of the user.

FIG. **12** is one embodiment of a flowchart illustrating one embodiment of a method for identifying account types of interest from groupings of transaction data items (for example, from the process of FIG. **11**). In some embodiments, the method of FIG. **12** may be performed by the account identification component **114**, whether operated by a account access system **202** or the account discovery system **110 A**. Depending on the embodiment, the method of FIG. **12** may include fewer or additional blocks and/or the blocks may be performed in order different than is illustrated.

Beginning at block **1210**, a payee included in the transaction data items is selected. For example, a payee that is associated with a grouping of multiple transaction data items (for example, 24 transaction data items spanning a period of 24 months of transaction data items) is selected.

Next, at block **1220**, rules for identifying a probable account type associated with the grouping of transaction data items are executed. Such rules may be stored in a datastore and/or in a rules engine. In some embodiments, the

payee identifier (for example, the normalized payee identifier) may be a significant factor in determining account type associated with the transaction data items. For example, is the normalized payee identifier is associated with a well-known wireless provider, designation of those transaction data items grouped with the wireless provider ID may be categorized as a wireless account without further application of account determination rules. In some implementations, even where a payee of multiple groups transaction data items is well-known, additional rules may be applied to the transaction data items, as well as the overall information derived at blocks **1130-1150**, for example, to validate that the grouping of transaction data items really is for the believed account type. For payee identifiers that are not well-known (for example, an account types is not readily known for a grouping of transaction data items associated with a particular payee), account identification rules may be applied.

Next, at block **1230**, a confidence level that a grouping of transaction data items is of a particular account type is determined. For example, at block **1220** a rule set for a rental account may be applied to the grouping of transaction data items and at block **1230** the confidence level that the grouping of transaction data items really is a rental account is determined. In some embodiments, the rules applied at block **1220** automatically output the confidence level of block **1230**, thus, these blocks may be combined in certain implementations.

At block **1240**, the account identification component **114** determines whether the confidence level calculated at block **1230** is above a threshold that indicates sufficient confidence that the selected account type accurately reflects the grouping of transaction data items. For example, if a rental account rule set is applied to the grouping of transaction data items at block **1220**, a confidence level that the grouping of transaction data items are associated with a rental account is determined at block **430**, and at block **1240** a confidence level threshold is compared to the confidence level calculated at block **1230** to determine if the transaction data items are associated with a rental account. In some embodiments, the threshold levels vary based on the account type. For example, a confidence level may be higher for rental account than for a wireless account.

If the confidence level is above the threshold at block **1240**, the method continues to block **1270** where the grouping of transaction data items are associated with the selected account type.

Depending on the embodiment, the confidence level associate with a grouping of transaction data items may be based on various information regarding the transaction data items, the financial account of the user, the financial institution from which the account information was obtained, the user (and/or related users, such as those in the same household), and/or other related characteristics. As an example, the account identification component **114** may determine if there are a sufficient number of transactions for the account to be reliable, may determine if the transactions were reported by a sufficiently reliable financial institution, and/or may determine if the transactions are consistent enough with patterns expected for such accounts (for example, rent transactions with amounts that vary each month may indicate a lower reliability that the transactions accurately reflect a rental account of the user, utility transactions with a payee name that doesn't match a known utility provider may indicate a lower reliability, and so forth). In some embodiments, the account identification component **114** may assign individual reliability scores to each of multiple factors, such as number

of transactions, reliability of the associated financial institution, consistency with typical patterns for such accounts, and so forth, and may combine the individual reliability scores to determine an overall reliability score. In some embodiments, a threshold confidence level may include both individual reliability scores for each of one or more individual factors and a an overall reliability score for all of the factors that are determinative of reliability.

If the confidence level is not above the threshold at block **1240**, the method continues to block **1250** where the account identification component **114** determines if additional information may be helpful in increasing the confidence level associated with the grouping of transaction data items. As an example, the account identification component **114** may determine that the account is a rental account and that obtaining a copy of the lease agreement would significantly improve the confidence of the system that the rental transactions are accurate, reliable, and properly associated with a rental agreement. As another example, the user account discovery system may determine that the account is a utility account and that confirming one or more details of the user's account directly with the utility provider would significantly improve the system's confidence in the utility account (for example, the account's reliability).

If additional information may be useful at block **1250**, at block **1280** additional information is requested from the user and/or a third-party. In some embodiments, information regarding transactions that may be missing in a grouping of transaction data items may be requested from the user and/or third-party to supplement the transaction data items acquired directly from the transaction provider and increase the confidence level. In some embodiments, the types of additional information and/or sources of additional mission may vary based on the account type being analyzed. In some embodiments, additional information may only be requested if the confidence level is already near the threshold, such as within 10% of the required confidence level.

As other examples, the user may be asked to provide the date and amount of a monthly rent (or other utility, wireless, or other) payment; the user may be asked to provide a copy of a lease agreement, a utility bill, or other such confirming information, the financial institution may be asked to provide additional details of the transactions, utilities may be asked to confirm account and/or transaction details, rental providers may be asked to confirm rental agreement details, and so forth.

If additional information is not needed at block **1250**, the account identification component **114** determines at block **1260** whether the grouping of transaction data items should be analyzed against other account types. For example, if the transaction data items are initially tested against rental account rules, at block **1260** the account identification component **114** may determine that utility account type rules should now be applied to determine whether those transaction data items are an utility account. If no additional account types are to be tested, the method continues to block **1290** where additional payees, or groupings of transaction data items associated with an additional payee, remain to be tested against the account type rules. If additional groupings of transaction data items do remain, the method continues to block **1210** where another grouping of transaction data items, associated with a particular payee, is selected and analyzed. At block **1295**, associations of transaction data item groupings with account types, as well as potentially the confidence levels associated with the identified account types, are stored for later access.

FIG. 13 is one embodiment of a flowchart illustrating an example of a method that may be performed to request additional information from third-party and/or from a user, such as may be performed at block 1250 and 1280 of FIG. 12. In the example of FIG. 13, at block 1310 the account identification component 114 determines sources and/or types of additional information that may be used to improve identification of accounts within categorized transaction data items. In some embodiments, the types of information that are helpful may be based primarily on the type of account being identified. For example, if a rental account is being identified (for example, a confidence level that a group of transaction data items are associated with a rental account of the user is met or almost met), a rental agreement between the user and the rental payee (for example, a landlord) may be the default data item requested of the user and/or third-party.

If a determination is made that additional information is requested from a third-party, at block 1320 a request for the additional information is transmitted to the third-party and at block 1330 the third-party provides additional information. Such additional information may include, for example, demographic information of the user that may be compared to information associated with a payee on the groups transaction data items to confirm that the user lives within a service district of the payee. If a determination is made that additional information is to be requested from the user, at block 1340 the information is requested from the user, such as via the mobile application or website with which the user is already interacting with the account discovery system, and the user provides requested additional information at block 1350. Examples of additional information that may be provided by a user could include a payment type (for example, cash, handwritten check, cashier check, and so forth), payment amount, digital images of payments, digital images of account specific information (for example, monthly invoices or statements from the payee), and so forth. In one example embodiment, the user is requested to provide a digital copy of at least a portion of a rental agreement to validate terms and existence of a rental account. Information from the rental agreement may be extracted, such as through an optical character recognition processing, to identify key terms of the rental agreement and compare such terms to information included in (or derived from) the grouping of transaction data items.

FIGS. 14-18 are example user interfaces that illustrate a user experience as the account discovery system accesses transaction data items of the user and attempts to identify accounts within the transaction data that can be added to the user's credit data. For example, the user interfaces may present dialogue blocks sequentially as the user interfaces with an artificial intelligence system (for example, provided by a credit bureau) that helps the user understand their credit situation better. For example, a user may click on certain of the dialogue blocks 1410 to cause additional dialogue blocks to be presented.

Beginning at FIG. 14, the dialogue blocks 1410 provide information to the user on types of accounts that may be used to increase the consumer's credit score, such as, for example, phone, Internet, a utility (for example, electrical, water, gas, and so forth) bills. The dialogue then continues to provide educational information regarding a payment history that may be needed to impact credit score the user. Depending on the embodiment, the payment history threshold for impacting a credit score of user may depend on the type of account. For example, a wireless account may be considered by a credit scoring algorithm with only three

months of consistent payment history, while a rental account may require six months. Different credit scoring algorithms may have different requirements, weightings, and factors, for example, for the required payment history for an account to be considered by the scoring algorithm.

FIG. 15 illustrates embodiments of additional dialogue blocks 1510 that provide current credit score information to the user, such as to provide a baseline to the user for comparison to a later calculated credit score, for example, after one or more new accounts are added to the credit data of the consumer. In this example, the dialogue blocks 1520 allow the user an option to watch a educational video describing how the user's DDA account information is accessed and analyzed to locate accounts of the user that can be added to the credit file of the user. Additionally, other educational videos or interactive media can be provided to the user.

FIG. 16-18 illustrate embodiments of additional dialogue blocks 1610-1810 that may be provided to the user, such as to educate user on additional areas related to their credit data. In some embodiments, the informational dialogue blocks, such as those in FIGS. 16, 17, and/or 18, may be presented to the user only while the account identification component 114 is still processing transaction data from the one or more links financial account of the user areas for example, after the account identification component 114 has completed processing of the transaction data items, presentation of further dialogue blocks may be postponed in favor of presenting the user with an indication of identified accounts for boosting the consumer's credit score, such as the dialogue block 1820 of FIG. 18.

FIG. 19-20 include embodiments of example user interfaces that may be presented to a user after scan of the consumer transaction data is completed and, in this example, accounts that may be added to the user's credit data are located. In other embodiments, the user interfaces may include additional or less information and/or may be formatted and presented in different manners. The user interfaces of FIGS. 19-20, as well as the other user interfaces discussed herein, are only examples of user interfaces that may present this information.

In some embodiments, the system may interact with the user via a chat window (for example, a pop-up window) that may be operated by a chatbot to request the information needed from the user and/or provide the user with educational information regarding the process. In some embodiments, such chatbots may be entirely automated (for example, using artificial intelligence that learns how to best interact with users over time) or may be partially operated by a human operator (for example, when the chatbot is unsure of how to respond to a query from the user). Similarly, any other user interactions discussed herein may be partially or fully performed via a conversational format, with a chatbot (for example, fully or partially automated) interacting with the user via primarily textual communications. FIGS. 14-18 illustrates example embodiments of such chat-like communications.

User interface 1910 request information from the user regarding a few potential accounts that could be added to the credit data of the consumer. The user interface request that the user confirm that payments to the identified payees are actually made by the user and, accordingly, could properly be used in calculating credit worthiness of the user. In this embodiment, if the user does not recognize payees listed, those payees can be removed by clicking the acts the right of the payee data identifiers.

After the user selects payees with which the user has an account, the user may select a confirmation indicator element, such as an “I make these payments” link or button, and be presented with a user interface **1920** which indicates that the account identification process performed by account identification component **114** (referred to loosely as a “scan” in certain of the user interface features discussed herein) has completed. The user interface further indicates that two accounts, of the type that may be added to credit data of users, have been identified. In this particular example, an electrical account (associated with the payee “So Calif Edison”) and a wireless account (associated with the payee “T Mobile”) have been identified.

User interface **1930** illustrates an example of a request for additional information from the user, in this case related to a potential lease account for which transaction data items were identified in the user’s transaction data. Advantageously, the user may launch a camera on their mobile application directly via the user interface **1930** and take one or more snapshots of the lease agreement. The lease agreement may then be processed by the account identification component **114** to validate a grouping of transaction data items associated with a lessee as indicative of a rental account of the user that may be added to credit data of the user.

FIG. **20** illustrates an embodiment of the user interface **2010** that provides detailed information regarding the transaction data items associated with a particular account, in this case the account associated with the payee “So Calif Edison” the example user interface identifies a number of payments that were found in the transaction data items, as well as an average payment amount across those located payments. In other embodiments, less or additional information regarding the individual transaction data items and/or data derived from all or some of the transaction data items, may be provided. In one embodiment, the user interface **2010** may additionally provide the account type associated with the identified payee, such as “utility account” associated with the identified payee “So Calif Edison.”

User interface **2020** includes further details regarding the payments that were found in the transaction data items. In this example, two years of prior data is illustrated graphically such that the user can identify months where they transaction data item was not located. In this example, April 2018 payment was not identified in the transaction data items. In some embodiments, the user is given an opportunity to update the account information with payments may outside of the linked DDA account. For example, the user may be given the opportunity provide a copy of a cashier’s check that was used to make the payment to So Calif Edison in April 2018 so that the historical payment activity for the account shows no missed payments over the last two years. Finally, after the user has reviewed information regarding the located account and related transaction data items, the user can select the “add to my credit file” button to initiate addition of the account to the user’s credit file.

FIG. **24A** is another embodiment of an example user interface that provides information regarding an identified account in transaction data items of user, with an option that is selectable by the user to add the account to credit data of the user (as a self-reported account). In the example of FIG. **24A**, the user interface may be displayed via a browser, such as on a desktop or laptop computer. However, the same or similar user interface may be displayed on any other display device or type. In this example, a payment account associated with So Cal Edison has been identified, and payments

identified in transaction data items are indicated in the payment history graphic **2412**. In this example, payments for two months in 2017 were not identified and a payment for one month in 2018 was not identified (indicated as gray circles in the payment history graphic **2412**, rather than green circles). Thus, 21 of 24 payments were identified in the prior two year history for the account. Missing payments in one or more calendar months may not necessarily indicate negative activity associated with the account. For example, a user may have made two payments within a given month (for example, paid bill on 1st and 31st of the same month), causing the following calendar month to not be associated with a payment. However, the payment for that following month was actually paid early, so the account identification component **114** may be programmed to identify special circumstances such as this example (either through manually provided rules and/or rules determined by machine learning) so missed payments can be more accurately identified.

Since there are a few missing payments, the user may want to review the payment transaction items that were identified by the account identification component **114** to determine if some of those missing payments can be located (for example, in another DDA account of the user). Similarly, the user may want to provide the account identification component **114** with additional information regarding payments made to the payee, such as an alternate payee identifier that may have been used in certain transaction data items. As another example, the user may want to authorize access to another DDA account where payments to the payee may also be located. Through these processes, the user may improve the payment history associated with the account and, accordingly, may further increase a score impact by addition of the account to credit data of the user. In some implementations, a user interface such as FIG. **24B**, which displays missing payments associated with a particular account, may not be displayed to the user until after the account is added as a trade line to the credit data of the user.

FIG. **24B** illustrates an embodiment of an example user interface **2420** that provides an overview of self-reported accounts that have been added to the credit data of the user. User interface **2420** may be considered to be an electronic, interactive view of the user’s credit report, and may provide the same or similar information that would be reported on a credit report delivered in other manners than a user interface. The user interface **2420**, or similar user interface, may be provided to third parties with a permissible purpose for viewing the consumers credit data. For example, a lender, landlord, or other entity interested in credit of a user, may view and electronic report of trade lines in the user’s credit data.

FIG. **24C** illustrates an embodiment of an example user interface **2430** that summarizes the various areas of consumer credit that may impact credit worthiness of the user. In this example, a current credit score interface **2431** is displayed, showing the user a relative strength of the current credit score of the user with how lenders may interpret that current credit score (for example, fair, good, very good, exceptional). This example also includes an account summary interface **2432** providing a summary of those accounts (for example, trade lines) that are currently part of the user’s credit data. In this example, self-reported accounts are identified separate from other credit accounts. In some embodiments, self-reported accounts may be combined with other credit accounts. The debt summary interface **2434** provides overall credit, retail, real estate, installment loan, and collections debt. The overall credit usage interface **2435** provides the user with an indicator of credit utilization

across all of the credit account of the user. Inquiries interface **2436** indicates the number of credit inquiries currently impacting credit score of the user, such as those that were received within the prior two-year period (or other time period, depending on the credit scoring algorithm). Public records interface **2438** indicates whether any derogatory public record information was identified for the user. The information summarized in user interface **2430** provides a user with a comprehensive overview of factors that generally weigh into credit score calculations, although each credit scoring algorithm may view these factors differently, may consider additional factors, and/or may not consider some of these factors.

The user interfaces of FIG. **24**, for example, may be utilized by the user as a form of financial account monitoring. Similarly, the information may be provided to the user and/or authorized third parties, in other formats, such as via periodic emails or push messages that summarize activity of the self-reported accounts of the user, as well as other credit data.

FIGS. **21-22** are conceptual diagrams illustrating example transaction data items that may be identified in transaction data of the consumer and analyzed to determine whether the groups transaction data items are indicative of an account that can be added to credit data of a consumer. In the example of FIG. **21**, transaction data items **2110-2118** represent five transaction data items that were identified in transaction data of a user in a DDA account of the user, each of which was associated with a common payee, "Big Landlord" in this example. As shown, the payments were each in the amount of \$475 and each occurred between 27 days and 33 days after the prior payment. Derived data **2120**, which indicates aggregated, summarized, extracted, and so forth data related to the transaction data items, is also illustrated in FIG. **21**. In the example transactions associated with Big Landlord, the account identification component **114** may determine, for example, that five payments were identified over a period of five months, the average payment amount was \$475, and the average days between payments was 31.25 days.

Also shown in the example of FIG. **21** are four transaction data items **2132-2138** that have each been associated with the payee "ABC Mobile". As shown, these example payments vary in amount from \$46 to \$118 and the time between payment varies from 27 days to 65 days. Thus, the derived data **2130** for the ABC Mobile transaction data items indicates an average payment of \$74.5 and average days between payments of 41.7 days. Another data point that may be derived from these transaction data items is the variance between payment amounts. In some implementations, rules for identifying a regularly recurring payment that is indicative of a wireless phone account may disqualify these transaction data items because of the large difference between the payment amounts (for example, between the \$46 and the \$118 payment amounts) and high average number of days between payments (for example, 41.7 days where an average of 30.4 days between payments is expected).

FIG. **22** illustrates the same transaction data items **2132, 2134, 2136, and 2138** associated with payee "ABC Mobile" as in FIG. **21**, but with additional analysis logic that splits the large payment **2136** of \$118 that was paid almost twice as many days from the prior payment **2134** as expected, into two simulated payments **2136A** and **2136B**. In this way, the account identification component **114** has interpreted the transaction data item **2136** in a way that causes the modeled number of payments to be 5, with the modeled average

payment being \$59.6, resulting in a much smaller variance between the low payment of \$46 and high payment of \$67, and the average days between payments of 31.25 days. Thus, this modeled data regarding the account may result in a much higher confidence level that the transaction data items are associated with a mobile account than application of the rules to the derived data **2130** of the original transaction data items.

Ongoing Access to Transaction Data Items

In some implementations, the account discovery system **110** periodically access transaction data items of the user, such as via the data permissioning component **112** that communicates with the financial institution of the user using the user security token. For example, the account discovery system **110** may periodically access recent transaction data items, for example, those transaction data items that are new since the financial account of the user was last accessed, to search for additional accounts of the user that could be added to the user's credit data. In some embodiments, the user is provided with a permissions dashboard that allows the user to selectively authorize uses of data associated with self-reported (and possible other) accounts of the user. For example, the user may opt into use of their credit data (including self-reported data) in calculation of other risk indicators and/or for other financial analysis or products. In one embodiment, the use can authorize use of credit data to calculate multiple risk indicators using various risk scoring algorithms. Some risk scoring algorithms may consider the self-reported accounts in the credit score calculation, while others may not directly consider the self-reported accounts in a credit score calculation, but may indirectly consider the accounts to the extent they impact the total debt, monthly payment obligations, equity, and so forth of the user.

FIG. **23** illustrates an embodiment of a user interface **2310** that may be provided to a user after an initial scan of transaction data items has been performed. User interface **2310** indicates that the financial information of the user is rechecked periodically to determine if additional accounts can be located for addition to credit data of the user. In some embodiments, the additional transaction data items are grouped with existing transaction data item groupings, such as those that were generated during an initial account identification process. Addition of new transaction data items to an existing grouping of transaction data items may increase a confidence level in identification of a particular account type such that the account is presented for confirmation by the user for addition to credit data the user. For example, an account with only two monthly payments in the initial transaction data item grouping may not be eligible for addition to credit data of the user, but over the next month when a third transaction data items indicating a third monthly payment associated with the payee is identified and associated with the payee, the grouping of transaction data items may meet the rules for addition of the account to credit data of the user.

Example user interface **2320** provides the user with example circumstances where further information may be available to identify accounts for addition to the user's credit data. In this example, the user is provided an opportunity to connect an additional account to the account discovery system **110**, such that additional transaction data items may be included in the account discovery process. For example, if the user previously authorized access to a checking account, the user may additionally authorize access to a savings account or another checking account at different

financial institution, to allow analysis of additional transaction data items that may be indicative of a utility, telecom, rental, and so forth account.

Example user interface **2330** is an example request the may be made to the user in an attempt to update payee information that may be indicated in transaction data items of the user (and/or other users). Such a request may be used to obtain data from the user that enhances the system's ability to identify transactions that the user can use to boost their credit score. In some embodiments, the user may be asked to provide examples of transactions that should qualify for the boost (for example, telecom and utility payments) and/or payee identifiers in transactions that are associated with a particular payee or type of payee. This user-provided information may then be used by the account identification component **114** to better identify transactions and accounts that could be added to credit data of the user.

In the example user interface **2330**, the user is requested to provide information regarding the specific payee ID that is used in the transaction name by the user's financial institution, where the specific payee ID used by the financial institution may differ from other payee IDs for the same payee that are used by other financial institutions and/or that are included in the payee database. Thus, the payee ID information provided by the user may then be added to the payee database and used when analyzing other user transaction data items to better match transaction data items from that particular financial institution and payee with the appropriate standardized payee identifier.

In some embodiments, the account identification component **114** periodically accesses additional transaction data items of the user and searches those transaction data items for new payment information associated with accounts that have previously been added to the user's credit data. For example, if a wireless account is added after an initial processing of transaction data items from a checking and savings account of a user added financial institution, those same checking and savings accounts of the user may be accessed monthly (or other time period) to search for new payments to the wireless account. After identifying payments to the wireless account, information regarding the new payment may be provided to the credit bureau as an update to status of the trade line. In this way, self-reported accounts may be added to credit data and updated on an ongoing basis with payment information, in a similar manner as traditional credit accounts are initially reported to the credit bureaus and updated with monthly payment information.

In some embodiments, ongoing access to transaction data items and providing updated payment information on self-reported tradelines may continue indefinitely. For example, as long as the account remains connected and the credentials remain active, the account discovery system may periodically access new transaction data items which may allow identification of new payments that meet criteria for addition of an account as a trade line, and user may be notified they have new boost available for them to use to increase their credit score.

Such ongoing access to transaction data items may allow new accounts for a boost to be identified as more payments are made to the corresponding payee. For example, if the user on initial scan only had one or two months of payment history identified for a particular payee, new transaction data items may be received over the following months to obtain the required threshold payment months for adding credit data. In this example, the user may be notified via email (or other communication medium) of the qualifying account

based on newly received transaction data items, and the account may be added to the user's credit data at the request of the user, or automatically upon identification (for example, if the user authorized later addition of the account when the initial scan was performed).

In some embodiments, the user provides permissions for later accesses to transaction information and/or may provide subsequent permissions to access the transaction information. In some embodiments, if a new payment for a tradeline has not been identified in transaction data items for more than a threshold time period (for example, three months, six months, and so forth), the self-reported tradeline may automatically be removed from credit data of the consumer. Additionally, as noted elsewhere, the user can remove permissions to periodically access transaction data at one or more financial institutions at any time.

In some embodiments, any disruption in monthly (or other periodic) updates to self-reported accounts, such as based on accessing transaction data items that one or more financial institutions in identifying payment information on those self-reported accounts, may trigger a notification to the user. For example, if a monthly scan of transaction data items from a DDA account (where a previous 12 months of payments on a self-reported account were identified) does not result in identification of a payment on the account, an alert may be transmitted to the user. For example, a text message, push notification, email, or other notification may be transmitted to the user device to alert the user of the missing payment. In some circumstances, the user may have inadvertently missed payment on the self-reported accounts and the notification provides the user with the ability to remedy the missed payment as quickly as possible. Alternatively, if the user purposefully missed payment, perhaps in conjunction with closing the account, the notification allows the user to indicate to the account discovery system that the self-reported accounts should be removed from credit data of the user. In some embodiments, alerts may be provided to the user based on other triggers, such as if credentials associated with a DDA account with financial institution have changed (for example, the transaction data items are no longer accessible by the account access system). Such an alert may request updated credentials (and/or new account information if the account has been canceled or transferred) from the user so that the system may be re-permissioned to access the transaction data items of the user account.

Example System, Method, and User Interfaces Associated with Trade Line Addition

FIG. **25** is an embodiment of a block diagram illustrating an account discovery system **2510** in communication with a financial institution **2500**, a user device **2520**, and a credit bureau **2530**. As noted above, the account discovery system **2510** may access financial account information of the user, after receiving permission from the user to access such financial account information, that may be analyzed to identify payments indicative of a self-reported account that may be added to the credit file of the user. In the embodiment of FIG. **25**, a vendor **2540**, such as a telecom, utility, or rental provider, receives payments from a user via a DDA account held with the financial institution **2500**. For example, the vendor **2540** may receive monthly checks from the user for wireless phone service. Such payments may be transmitted electronically to the vendor **2540** or in paper form, such as by checks automatically printed and transmitted from the financial institution **2500** or checks that are handwritten by the user. In this embodiment, the account discovery system **2510** initially communicates with the user device **2520**, to receive authorization from the user to access

account information of the user with the financial institution **2500**, such as using processes described elsewhere herein. With the appropriate authorization in place to access the financial account data of the user at the financial institution **2500**, transaction data items of user are accessed via a secure communication channel with the financial institution **2500**. The identified accounts within the transaction data items (for example, as defined by the account identification component **114**), may be validated by the user and then added to the credit data of the consumer as a trade line that is usable by credit scoring algorithms in calculating the credit score of the user. As shown in FIG. **25**, account discovery system **2510** transmits a new trade line request to the credit bureau **2530**, such as in a particular format that is understandable by the credit bureau **2530**. Additionally, communications from the account discovery system **2510** with the credit bureau **2530** may occur periodically, such as to provide additional new trade line requests (for example, for accounts that are identified as additional transaction data items are processed by the account discovery system **2510**) and to add additional payment information to the consumer's credit data for trade line that have previously been added by the account discovery system **2510**. In this way, the account discovery system **2510** provides up-to-date transaction data to the credit bureau **2530** that allows the user's credit history to grow over time as payments are made to the vendor **2540**.

FIG. **26** is an embodiment of a flowchart illustrating one embodiment of a method of providing a new trade line request to a credit bureau to initiate addition of a self-reported account to credit data of the user. Defendant embodiment, the method of FIG. **26** may include additional or fewer blocks and/or the blocks may be performed in order different than is illustrated. Beginning in block **2610**, a request update credit data of a user is received from a user computing device. The request is particularly for self-reported accounts of the user, such as rental, utility, and telecom accounts, among others. In block **2620**, after the account discovery system has identified a self-reported account to be added to the user's credit data (for example, using processes discussed herein associated with the data permissioning component **112**, the account identification component **114** and/or the account verification component **116**), a new trade line data package is prepared for transmission to a credit bureau. In embodiments where a new trade line request is provided to multiple credit bureaus, multiple new trade line data packages may be prepared, one for each credit bureau, formatted and including information that may be specific to the particular credit bureau for purposes of adding a new trade line to the user's credit data. Next, at block **2630**, the specially prepared trade line creation data packages transmitted to the credit bureau. Advantageously, the trade line creation data package may be formatted in the same manner as a new trade line creation data package for a traditional credit account, such as a credit card or loan. Thus, the credit bureau may as the new trade line to credit data of the consumer and the credit data may be immediately usable by credit scoring algorithms.

FIG. **27** illustrates an embodiment of example user interfaces associated with addition of a new account to credit data of the user. Example user interface **2710** may be provided to a user after the user confirms that a newly identified account should be added to the user's credit data. In other embodiments, the addition of the new trade line to credit data of the consumer may be instantaneous (for example, completing in a few seconds) or may take a bit more time, such as tens of seconds or even a few minutes.

As noted above, after the new trade line has been added to the user's credit data, that new trade line is immediately usable by credit scoring algorithms. User interface **2720** illustrates a scoring interface that may be displayed to the user shortly after addition of a new trade line to the user's profile. For example, after the user selects and identified account to be added as a trade line to credit data of the user, the new trade line creation data package may be prepared and sent to the credit bureau (and a user interface such as user interface **2710** may be provided to the user), and in response to confirmation that the new trade line has been added to the credit data of the user a scoring algorithm may be executed on the updated credit data of the user to generate an updated credit score. In the example of FIG. **27**, user interface **2720** indicates that, after addition of the new trade line to the user's credit data, the users credit score has increased by 22 points to a score of 691. In some embodiments, a user interface similar to user interface **2720**, in addition to or instead of indicating a number of points that the credit score increased, may indicate a change in score band for the credit score, such as by indicating that the added tradeline(s) increased the user's credit score from a "fair" score band to a "good" score band. Accordingly, by optimizing communications between multiple devices, obtaining proper authorizations from the user, and for dating with credit bureaus for additions and data scoring based on new account information, the systems discussed herein provide the user with an advantage that has not previously been available.

FIG. **28A** illustrates embodiments of example user interfaces that may be provided to a user to indicate availability of additional product offers, such as credit offers, in view of an increase credit score, such as may be caused by the addition of a new self-reported account to credit data of the user. For example, a credit card matching service, such as Experian's CreditMatch, may interface with the Account Discovery System to obtain updated credit scores of users which may then be used to qualify the user for additional credit offers. In example user interface **2810**, a message **2812** indicates that additional credit card offers have been associated with the user in view of the 22 point increase in the consumer's credit score. For example, a credit card matching system may consider a credit score of a user as an important factor in whether a user qualifies for a particular credit card. Thus, with a credit score increase, such as the example increase of 22 points illustrated in example user interface **2810**, the user may qualify for multiple credit card offers for which the user did not qualify previous to the 22 point increase. User interface **2820** similarly illustrates a particular credit card offer for which the consumer qualifies after the 22 point credit score increase, which the consumer did not qualify for prior to the credit score increase.

FIG. **28B** illustrates an embodiment of an example user interface **2830** that may be provided after the consumer has boosted their credit file by adding one or more self-reported accounts. As shown in user interface **2830**, information regarding newly available credit offers **2832** and **2834** is provided to the user. In this embodiment, the user did not qualify for the credit offers **2832** and **2834** prior to addition of a self-reported account, but after a self-reported account was included in tradeline data of the user, the credit score of the user increased and moved above a threshold minimum credit score requirements for credit offers **2832** and **2834**.

FIG. **28C** is an embodiment of an example user interface **2840** that may be provided to the user as part of an online credit report that is accessible to the user, either through a free or paid account with a credit reporting agency or other

authorized credit reporting entity. In this example, the user has selected a newly added “utility self-reported” account and detailed information regarding that self-reported account is provided in user interface **2840**. In some embodiments, and account detail page similar to user interface **2840** may be provided to a user immediately after addition of a new self-reported account. In the example user interface **2840**, an account management button **2842**, is provided to direct the user to an account dispute page where the user will have the option to remove the self-reported account from credit data. For example, selection of account management button **2842** may direct the user to a dispute center user interface, such as the example illustrated in FIG. **37**.

FIG. **28D** is an embodiment of another example user interface **2850** that may be provided to the user as part of an online credit report. Example user interface **2850** provides summary information of the self-reported accounts currently associated with the credit data of the user. In this example, information regarding to utility self-reported accounts, rent self-reported account, and a telecom self-reported account are displayed. The “View” element associated with the self-reported accounts may be selected to direct the user to an account detail page, such as the example user interface **2840** of FIG. **28C**.

Removal of Added Trade Lines

In some implementations, addition of new trade line to the user’s credit data may not have the desired effect on credit score of the user. For example, in some situations, addition of a new trade line may actually cause the credit score of the user to decrease, or to not change at all. Accordingly, in some embodiments, the account discovery system **110** provides a mechanism allowing the user to remove any previously added self-reported trade line from their credit data.

In some implementations, an improvement to the credit situation of a user may be realized through addition of self-reported accounts, even if the credit score of the user decreases or stays the same. For example, a user’s overall credit health could be seen as improving if addition of a self-reported account increases the total number of trade lines above a thin file threshold (for example, four or more trade lines) so that the user is seen as a thick file user. Thus, while a credit score increase is a straightforward indicator of credit health of a user, other factors associated with creditability of the user may also be considered by potential lenders, landlords, partners, and so forth. Accordingly, in some embodiments, the accounts discovery system provides educational material to the user, such as when their credit score has not increased responsive to a boost (or has actually decreased responsive to a boost), so that the user has an option to either remove the self-reported account or to maintain the self-reported account in the user’s credit data because of an advantage in overall creditability of the user with the newly added self-reported account.

FIG. **29** provides embodiments of example user interfaces that may be used in a trade line removal process. The example user interface **2910** explains that the credit score of the user decreased by eight points due to addition of a new trade line (for example, that was identified by the account discovery system in transaction data items of a DDA account of the user). Furthermore, the user interface **2910** provides a brief explanation of why addition of the new trade line caused a drop in credit score of the user. For example, a credit score may decrease if a new account(s) increased debt of the user.

Example user interface **2920** provides additional information to the user regarding reasons that newly added accounts that have caused the credit score of the user to drop

may still be beneficial to keep in credit data of the user. For example, user interface **2920** explains that the credit file of the user is being evaluated different now that it has additional trade line’s, which may allow the user to qualify for additional offers even with a lower credit score. User interface **2930** further explains that lenders won’t see newly added positive bill payments in the trade line that was added by the account discovery system, but that the user’s credit score will go back up when the trade line is removed.

Should the user decide to remove one or more self-reported accounts that have been added by the account discovery system, such as by selecting user interface element **2912** or **2932**, removal of the recently added account from the credit data of the user is initiated. Thus, users can remove accounts added through the account discovery system and their credit score will revert to the same score they had prior to addition of the new trade line. If the user continues to pay their utility and telecom bills on time to build positive payment history, they may later use the credit score update features again to recalculate their (hopefully increased) score,

FIG. **36** illustrates an embodiment of an example user interface **3610** that may be provided to a consumer who wishes to stop periodic reporting of payment activity for one or more self-reported accounts. Example user interface **3610** may be provided to the user in response to the user’s request to stop reporting transaction data items associated with a particular pay the (for example, “So Calif Edison” an example of FIG. **36**). The user interface provides information detailing how this may impact the credit file and/or the credit score of the user. The user is provided with an option to keep the trade line in the user’s credit data or to remove the trade line from the user’s credit data.

Example System, Method, and User Interfaces Associated with Updating Offers to the User

FIG. **30** is an embodiment of a flowchart illustrating one embodiment of a method that may be performed to provide updated offers to a user responsive to an increase in credit score of the user that is caused by addition of one or more self-reported accounts to credit data of the user. In some embodiments, the method of FIG. **30** may be performed by an offer provider, such as a credit card prescreening and/or prequalification provider, that provides credit card offers to consumers for which the consumers are likely qualified, such as based on lender criteria that may rely heavily on credit score of users. In other embodiments, the method of FIG. **30** may be performed by a credit risk agency, such as a credit bureau, that partners with credit issuers to provide prescreened credit offers as soon as possible after a consumer’s credit score has changed. In other environments, the method may be performed by multiple entities and/or systems, or other entities or systems that provide other offers to consumers. Depending on the embodiment, the method of FIG. **30** may include fewer or additional blocks and/or the blocks may be performed in order different than is illustrated.

Beginning at block **3000**, the offer provider determines identification information of a user, such as information that is usable to obtain a credit score of the user. In block **3010**, a current risk score of the user is obtained and/or calculated. For example, identification information obtained at block **3000** (for example, first name, last name, address, Social Security number, and so forth) may be provided to a consumer reporting agency with a request for a current credit score of the user. If the offer provider has the necessary permissible purpose for obtaining credit data of the

user, the consumer reporting agency will calculate and return a current credit score of the user.

Moving to block **3020**, the offer provider determines a first one or more product offers available to the user based on the current risk score. For example, each of multiple credit card offers (or automobile loans, home loans, or other offers) may be associated with a minimum credit score that qualifies users for the particular credit card offer. Thus, the credit score of the user may disqualify the user from eligibility for certain credit offers. Similarly, the credit score of the user may qualify the consumer for a first one or more credit offers (for example, those credit offers having eligibility criteria including a minimum credit score that is lower than the current credit score of the user). Accordingly, the offer provider may determine a first set of offers that the user is eligible to receive (and which the user may ultimately qualify for after full application) at block **3020** and a second set of offers that the user is not ineligible to receive (and for which the user would ultimately not qualify for after full application) at block **3030**.

Next, at block **3040**, the offer provider provides the user with an option to initiate updates to risk data of the user, such as by allowing the user to interface with the account discovery system to potentially identify self-reported accounts that could be added to credit data of the user to increase the user's credit score. In response to the user selecting the option to initiate updates to credit data, at block **3050** the offer provider initiates communication between the user and the account discovery system. The user may then interface with the account discovery system to provide the necessary permissions to access financial data, validation of account information, and confirmation that located accounts may be added to the user's credit data.

Next, at block **3060**, the account discovery system may automatically provide an updated credit score of the user to the offer provider, such as by requesting execution of a credit scoring algorithm on credit data of the user after a new trade line creation data package has been transmitted to the credit bureau. In other embodiments, after the account discovery system has interfaced with the user, a notification may be transmitted to the offer provider indicating that a new credit score of the user may be requested again. In such case, the offer provider may obtain an updated risk score of the user with a similar process as described above with reference to block **3010**.

At block **3070**, with the newly calculated credit score of the user, the offer provider identifies one or more of the second set of product offers (which the user was not eligible for previously) for which the user is now qualified. For example, if the user's credit score increased from 650 to 680 based on one or more added trade line's by the account discovery system, the user would not have qualified for a credit card requiring a credit score of 660 prior to the score increase, but would qualify for the credit card after the score increase (assuming the user meets any other eligibility requirements for the credit card).

At block **3080**, the new credit offers for which the user now qualifies are provided to the user, so that the user can potentially apply for any of the first set of credit offers and/or any of the newly identified credit offers from the set.

FIG. **31** is an embodiment of an example user interface that may be provided by and offer provider, such as an offer provider that prescreens users for credit card offers and provides information regarding matching credit cards to the user. In the example of FIG. **31**, the user has already engaged the account discovery system and received an increase in credit score. As indicated by text box **3110**, a "new offer" is

displayed to the user, where that particular credit card offer was not displayed to the user prior to the credit score increase initiated by addition of a new trade line to the credit data of the user.

FIG. **32** includes embodiments of example user interfaces that may be displayed on a mobile device of a user to invite the user to engage the account discovery system to potentially increase the credit score of the user and potentially allow more offers to be provided to the user. Example user interface **3210** may be triggered based on upcoming travel activity associated with the user. For this example, the user is invited to explore addition of new trade line to credit data of the user in order to increase the user's credit score and potentially qualify for a credit card that provides better mileage benefits.

The example user interface **3220** is provided to a user after detecting that the user does not have a credit score yet, which could be the case for teenagers or young adults, retired persons, ex-patriots, and so forth. With the availability of self-reported accounts to credit data of users, establishment of a credit report having one or multiple trade lines, as well as a corresponding credit score, may be significantly simplified. For example, payment history for a rental property over the course of many months or years may very quickly be added to credit data of the user.

The example user interface **3230** is provided to a user in response to the user applying for credit, perhaps prior to the user finalizing and agreement for credit. In this example, the user may increase their credit score by adding self-reported accounts to their credit data and thereby become eligible for a better credit offer than the one they previously applied for. In other embodiments, other triggers for providing invitations to explore addition of nontraditional accounts to credit data of users may be used.

System, Method, and Example User Interface Associated with Calculating Expected Score Increase

FIG. **33** is an embodiment of a flowchart illustrating one embodiment of a method that may be performed by the account discovery system to provide users with an estimated score increase that they may expect prior to adding new trade lines to their credit file. Depending on the embodiment, the method of FIG. **33** may include few or additional blocks and/or the blocks may be performed in order different than is illustrated.

Beginning at block **3310**, a score impact rule indicating a plurality of account types impacting credit scores of users may be accessed. For example, the score impact rule may indicate that rental accounts, water accounts, and electrical accounts impact credit scores of users, while country club accounts do not impact credit scores of users.

At block **3320**, credit data of a user is accessed, such as information regarding current trade lines and trade line types included in credit data of the user.

Next, at block **3350**, the score impact rule is applied to the determined account types already in the user's credit data to identify any account types that are not already in the user's credit data. For example, if the user's credit data does not already include an electrical account, electrical account may be identified at block **3350** as a potential new account type that could be added to credit data of the user to increase credit score of the user. In one embodiment, an expected score impact may be calculated for each multiple account types, regardless of whether the user already has an account of any of the account types.

At block **3360**, a score impact algorithm may be executed to determine a possible credit score change if an account of the identified account type is added to the credit data of the

user. For example, with reference to the example above, the score impact algorithm may calculate a numerical credit score change that is possible if the user adds an electrical account to the user's credit data. For example, the score impact algorithm may be based on a model developed through analysis of a plurality of users each having added electrical accounts to credit data, such as via the account discovery system or similar system for identifying and adding self-reported accounts to consumer credit data. Thus, the score impact algorithm may estimate, based on realized credit score changes by those other users that also added an electrical account to their credit data, an expected credit score change for the particular user.

In some embodiments, the score impact algorithm considers other factors, such as demographic information of the user as compared to the base set of users from which the model was generated, in calculating the potential credit score change. For example, if users in general experienced a credit score increase of 12 points by addition of a rental account to their credit data, but users in northern California experienced a credit score increase of 24 points by addition of a rental account to their credit data, the calculated credit score change may be impacted based on the location of the rental unit associated with the rental account. Similarly, the score impact algorithm may vary based on number of trade line's already in the user's credit data, outstanding balances, public record information, and so forth, where, in general, the more similar a user is to a group of users that previously added an account of the same type to their credit data, the more similar the possible credit score change for the particular user will be to that group of users.

FIG. 34 includes embodiments of example user interfaces that may be provided to users to indicate possible credit score changes. Depending on the implementation, information already known about the user, and other factors, the level of specificity provided in the possible credit score change provided to the user may vary.

In the example user interface 3410, the user is notified that addition of a utility account to credit data of the user would potentially increase the user's credit score. In one embodiment, this message is provided to the user based on a determination that the user does not already have a utility account in credit data of the user. Additionally, in some embodiments the notification may only be provided if the user has the right quantity of other trade line, outstanding debt balances, and so forth, in their existing credit data, such that addition of the identified account type would actually increase the credit score of the user.

Example user interface 3420 indicates that an expected credit score increase of 22 points could be possible for the user with the addition of six months of consistent rental history. In one embodiment, the notification may be based on little information regarding the user, such as perhaps only a geographic location of the user, while in other embodiments the possible credit score change may be more precisely based on additional known information of the user, such as that the user has three trade lines on their credit report already, but no rental account in their credit data. As another example, a more precise estimate could be developed based on information associated with existing credit data of the user, such as payment history, how much each monthly payment affects their overall balance, if addition of a new tradeline would cause the credit file to move from a thin file to a thick file, and other attributes of the user's credit data.

Example user interface 3430 indicates that 87% of people with a credit file similar to the user saw an increase in their

credit score with a boost (for example, with an addition of a new self-reported account to credit data of the user). In this example, the credit scoring algorithm may consider multiple attributes of the user in identifying a group of other users from which to calculate a likelihood of a credit score increase. For example, other users with a similar credit score (prior to boost), a similar quantity of trade lines, a similar amount of credit utilization, in a similar geographic region, and/or other factors, may be the basis for estimating how a new self-reported account might impact credit score of the user. In some embodiments, such estimations may be based on analytics of other users with similar credit files who have leverage the boost product (and/or other data indicative of changes to credit scores responsive to addition of self-reported accounts). FIG. 35 illustrates an embodiment of another example user interface that displays a similar estimate of credit score increase likelihood.

In one embodiment, the system provides an interactive score simulator interface that allows the user to be provided with real-time estimates of credit score changes in response to selection of hypothetical updates to credit data. For example, at block 3350 of FIG. 33, a user may identify a particular account type that could be added to the user's credit data and the system would determine an estimated score impact. In one example implementation, a simulator interface may allow the user to select one or more of a plurality of account types (for example, utility, rental, telecommunication, etc.) and, in response, be provided with an estimated credit score change for the selected account type(s). The estimated credit score change may be in various formats, such as an expected updated credit score, an expected credit score increase (or decrease), a direction of expected credit score change, and/or other indicators. In some embodiments, further details regarding accounts that may be added to credit data of the user may be provided to allow the system to generate a more precise estimated credit score change. For example, in addition to selection of a particular account type (for example, cell phone account), the user may provide other hypothetical information, such as number of on-time monthly payments, number of missed payments, range of monthly payments, etc. that may be used by a score impact algorithm provide more accurate estimated risk scores. Thus, a user may be provided with a first estimated risk score increase of zero for addition a first account type with 11 monthly payments, but a second estimated risk score increase of more than zero for addition of the same first account type with 12 monthly payments. Accordingly, the system provides information on account details for increasing credit scores as well as the general account types that may be added to increase credit scores.

In some embodiments, multiple estimated credit scores are provided simultaneously to the user, such as an estimated risk score associated with addition of each of multiple account types. The user may then be able to select an account type, such as one that has the highest estimated risk score increase, to initiate addition of transaction data associated with an account of the selected account type, such as using the systems and methods discussed herein.

Disputing Self-Reported Account Information

FIG. 37 is an embodiment of an example user interface that may be provided to the user that wishes to dispute information associated with a self-reported account, such as an account that is added as a trade line to credit data of the user by the account discovery system discussed herein. In one embodiment, any dispute to information in a self-reported trade line can be resolved by removal of the trade line from credit data of the user. In other embodiments, a

user may be provided the ability to update the transaction data items used in developing the trade line overview or to fill in missing payments that may be negatively impacting the user's credit data.

System Block Diagram

FIG. 38 is a block diagram illustrating one embodiment of an account discovery system 3802 that may be used to implement certain systems and methods discussed herein, such as providing a credit report to a user, gathering transaction data regarding non-traditional credit accounts of users, verifying account information with the user, adding the accounts as a self-reported accounts in the credit data of the user, and updating users' credit scores based on newly added self-reported accounts.

In one embodiment, the account discovery system 3802 is configured to interface with multiple devices and/or data sources. The account discovery system 3802 may be configured to implement certain systems and methods described herein. The functionality provided for in the components and modules of the account discovery system 3802 may be combined into fewer components and modules or further separated into additional components and modules. The account discovery system 110, account discovery system 110A, and/or the account access system 202 may include the same or similar components as illustrated in FIG. 38.

In general, the word component or module, as used herein, refers to logic embodied in hardware or firmware, or to a collection of software instructions, possibly having entry and exit points, written in a programming language such as, for example, C, C++, C#. A software module may be compiled and linked into an executable program, installed in a dynamic link library, or may be written in an interpreted programming language such as, for example, BASIC, Java, Perl, or Python. It will be appreciated that software modules may be callable from other modules or from themselves or may be invoked in response to detected events and interrupts, or both. Software instructions may be embedded in firmware, such as an EPROM. It will be further appreciated that hardware modules may be comprised of connected logic units, such as programmable gate arrays or processors. The modules described herein are preferably implemented as software modules, but may be represented in hardware or firmware. Generally, the modules described herein refer to logical modules that may be combined with other modules or devices into sub-modules despite their physical organization or storage.

In one embodiment, the account discovery system 3802 includes, for example, one or more servers or personal computers that are IBM, Macintosh, or Linux/Unix compatible. In another embodiment, the account discovery system 3802 includes one or more laptop computers, smart phones, personal digital assistants, or other computing devices. The account discovery system 3802 may include a memory 3830, which may include a random access memory (RAM) for temporary storage of information, a read only memory (ROM) for permanent storage of information, and/or a mass storage device, such as a hard drive, diskette, optical media storage device, or USB flash drive. Typically, the modules of the monitoring system are in communication with each other via a standards based bus system. In different embodiments, the standards based bus system could be Peripheral Component Interconnect (PCI), Microchannel, SCSI, Industrial Standard Architecture (ISA), and Extended ISA (EISA) architectures, for example.

The account discovery system 3802 may be generally controlled and coordinated by operating system software, such as Windows 95, 98, NT, 4000, XP, Vista, 7, 8, SunOS,

Solaris, Blackberry OS, or other compatible operating systems. In Macintosh systems, the operating system may be any available operating system, such as MAC OS X. In other embodiments, the account discovery system 3802 may be controlled by a proprietary operating system. Conventional operating systems control and schedule computer processes for execution, perform memory management, provide file systems, networking, and I/O services, and provide a user interface, such as a graphical user interface (GUI), among other functions. The example account discovery system 3802, as well as the account discovery system 110 shown in FIGS. 2A and 2B, may include one or more commonly available input/output (I/O) interfaces and devices 3811, such as a keyboard, mouse, touchpad, and printer. In one embodiment, the I/O interfaces and devices 3811 include one or more display devices, such as a monitor, that allow the visual presentation of data to a user. More particularly, a display device provides for the presentation of GUIs, application software data, and multimedia presentations, for example. The account discovery system 3802 may also include one or more multimedia devices 3840, such as speakers, video cards, graphics accelerators, and microphones, for example. In one embodiment, the I/O interfaces and devices 3811 comprise devices that are in communication with modules of the account discovery system 102 via a network, such as the network 3860, or any local area network, including secured local area networks, or any combination thereof. In the embodiment of FIGS. 2A and 2B, for example, the account discovery system 3802 also includes components that may be executed by the CPU 3805. The account discovery system 3802 is configured to gather credit data about users. The credit data, which may be stored in mass storage device 3820, may include the user's credit report as well as one or more credit scores for the user, such as a FICO score, a credit score proprietary to a particular credit bureau, and/or a multi-bureau credit score, such as a VantageScore. In some embodiments, the credit score that is used by the account discovery system 3802 advantageously considers rental payment history (for example, history of rental payments for a residence of the user) and/or utility payment history (for example, history of payments to utilities providers such as gas service, electric service, and telephone service providers) in generated credit scores. Thus, in such embodiments the credit score is weighted based on the rental payment history and/or the utility payment history of the user. Credit data, which may be stored in mass storage device 3820, may also include data not typically on credit reports such as the user's income, rental payments, utility payments, or other financial information about the user, such as may be obtained using the systems and methods described herein.

The account discovery system, client computing devices, financial institutions, service providers (for example, rental service providers, telco service providers, utility service providers, and so forth) may communicate with each other over network 3860. Network 3860 may be formed from one or more networks including any combination of wired networks, wireless networks, wide-area networks such as the Internet, and local-area networks.

Additional Embodiments

It is to be understood that not necessarily all objects or advantages may be achieved in accordance with any particular embodiment described herein. Thus, for example, those skilled in the art will recognize that certain embodiments may be configured to operate in a manner that achieves or optimizes one advantage or group of advantages

as taught herein without necessarily achieving other objects or advantages as may be taught or suggested herein.

All of the processes described herein may be embodied in, and fully automated, via software code modules executed by a computing system that includes one or more computers or processors. In some embodiments, at least some of the processes may be implemented using virtualization techniques such as, for example, cloud computing, application containerization, or Lambda architecture, and so forth, alone or in combination. The code modules may be stored in any type of non-transitory computer-readable medium or other computer storage device. Some or all the methods may be embodied in specialized computer hardware.

Many other variations than those described herein will be apparent from this disclosure. For example, depending on the embodiment, certain acts, events, or functions of any of the algorithms described herein can be performed in a different sequence or can be added, merged, or left out altogether (for example, not all described acts or events are necessary for the practice of the algorithms). Moreover, in certain embodiments, acts or events can be performed concurrently, for example, through multi-threaded processing, interrupt processing, or multiple processors or processor cores or on other parallel architectures, rather than sequentially. In addition, different tasks or processes can be performed by different machines and/or computing systems that can function together.

Conditional language such as, among others, “can,” “could,” “might” or “may,” unless specifically stated otherwise, are understood within the context as used in general to convey that certain embodiments include, while other embodiments do not include, certain features, elements and/or steps. Thus, such conditional language is not generally intended to imply that features, elements and/or steps are in any way required for one or more embodiments or that one or more embodiments necessarily include logic for deciding, with or without user input or prompting, whether these features, elements and/or steps are included or are to be performed in any particular embodiment.

Disjunctive language such as the phrase “at least one of X, Y, or Z,” unless specifically stated otherwise, is understood with the context as used in general to present that an item, term, and so forth, may be either X, Y, or Z, or any combination thereof (for example, X, Y, and/or Z). Thus, such disjunctive language is not generally intended to, and should not, imply that certain embodiments require at least one of X, at least one of Y, or at least one of Z to each be present.

Any process descriptions, elements or blocks in the flow diagrams described herein and/or depicted in the attached figures should be understood as potentially representing modules, segments, or portions of code which include one or more executable instructions for implementing specific logical functions or elements in the process. Alternate implementations are included within the scope of the embodiments described herein in which elements or functions may be deleted, executed out of order from that shown, or discussed, including substantially concurrently or in reverse order, depending on the functionality involved as would be understood by those skilled in the art.

Unless otherwise explicitly stated, articles such as “a” or “an” should generally be interpreted to include one or more described items. Accordingly, phrases such as “a device configured to” are intended to include one or more recited devices. Such one or more recited devices can also be collectively configured to carry out the stated recitations. For example, “a processor configured to carry out recitations

A, B and C” can include a first processor configured to carry out recitation A working in conjunction with a second processor configured to carry out recitations B and C.

The term “remote” may include data, objects, devices, components, and/or modules not stored locally, that are not accessible via the local bus. Thus, remote devices may include a device which is physically stored in the same room and connected to the user’s device via a network. In other situations, a remote device may be located in a separate geographic area, such as, for example, in a different location, country, and so forth.

Many variations and modifications may be made to the above-described embodiments, the elements of which are to be understood as being among other acceptable examples. All such modifications and variations are intended to be included herein within the scope of this disclosure.

What is claimed is:

1. A method performed by a computing system having one or more hardware computer processors and one or more non-transitory computer readable storage devices storing software instructions executable by the computing system to perform the method, the method comprising:

receiving, from a user computing device of a user, a selection of a third-party entity;

identifying an Application Programming Interface (API) token associated with the third-party entity;

transmitting the API token to a system in electronic communication with the third-party entity;

receiving, via the system, indicators of one or more accounts of the user with the third-party entity;

receiving, from the user computing device, a selection of an account of the one or more accounts;

accessing, via a secure communication session initiated with the API token, a plurality of data items of the selected account of the user with the third-party entity;

transmitting first user interface data to the user computing device, the first user interface data configured to depict a first user interface on a display of the user computing device, the first user interface including one or more interactive elements selectable to indicate authorized uses of the data items by the computing system;

receiving, from the user computing device, a selection of authorized uses of at least a subset of the data items;

and

in response to receiving the selection of authorized uses, selectively sharing at least the subset of the data items with a computing device for the one or more authorized uses, wherein the computing device is different than the user computing device and the computing system.

2. The method of claim 1, wherein selectively sharing at least the subset of the data items is with one or more third parties.

3. The method of claim 1, wherein the method further comprises:

transmitting second user interface data to the user computing device, the second user interface data configured to depict a permissions interface element that is selectable to indicate authorization to access account information associated with the user; and

receiving, from the user computing device, authorization to access the account information associated with the user.

4. The method of claim 1, wherein the method further comprises:

receiving credentials for accessing account information associated with the user at the third-party entity, and

receiving, from the user computing device, authorization to access the account information associated with the user.

receiving, from the user computing device, authorization to access the account information associated with the user.

receiving, from the user computing device, authorization to access the account information associated with the user.

receiving, from the user computing device, authorization to access the account information associated with the user.

receiving, from the user computing device, authorization to access the account information associated with the user.

receiving, from the user computing device, authorization to access the account information associated with the user.

transmitting, to the system in electronic communication with the third-party entity, the credentials.

5. The method of claim 4, wherein the first user interface includes an iframe provided by the system in electronic communication with the third-party entity, wherein the credentials are provided directly to the system in electronic communication with the third-party entity.

6. The method of claim 4, wherein the credentials are not stored by the computing system.

7. The method of claim 4, wherein the credentials comprise one or more of (1) a username and password, or (2) biometric data of the user.

8. The method of claim 4, wherein the system in electronic communication with the third-party entity stores the credentials for use in a later request for information associated with the user from the third-party entity.

9. The method of claim 1, wherein data items associated with a post date more than a predetermined number of years prior to a current date are disregarded.

10. The method of claim 1, wherein the system in electronic communication with the third-party entity communicates with the third-party entity via a secured API communication channel initiated via use of a second API token associated with the third-party entity.

11. The method of claim 1, further comprising:

accessing the plurality of the data items;

selecting a first data item of the plurality of data items;

determining a recipient identified in the first data item;

identifying a subset of data items each indicating the determined recipient, wherein the subset of data items includes at least the first data item and one or more other data items;

determining, based at least on the identified subset of data items, account data associated with an account of the user associated with the recipient, the account data comprising at least one or more of:

a number of data items each having time stamps within a predetermined time period; or

average number of days between time stamps of sequential data items;

applying a first account identification rule, associated with a first account type, to the account data;

determining, based on said application of the first account identification rule, a first confidence level indicating likelihood that the account is of the first account type; and

in response to determining that the first confidence level is about a first threshold, applying a first account scoring model to the account data, the first account scoring model configured to determine an expected change to a current risk score associated with the user.

12. The method of claim 11, further comprising:

receiving, from the user computing device, confirmation that the account of the user is of the first account type;

receiving, from the user computing device, a request to add the account with the recipient to risk data associated with the user at a secured third-party risk database;

generating, based on portions of the plurality of data items and the account data associated with the recipient, an account creation data package, the account creation data package formatted for ingestion at the secured third-party risk database to initiate addition of the account to risk data of the user;

identifying a security key associated with the secured third-party risk database; and

transmitting the security key and the account creation data package to the third-party risk database via a secure communication channel established with the third-party risk database.

13. The method of claim 12, further comprising:

requesting execution of a risk scoring algorithm using risk data of the user at the secured third-party risk database, wherein the risk scoring algorithm is based at least partly on portions of the plurality of data items or the account data included in the risk data of the user; and providing risk score change information to the user computing device.

14. A computing system comprising:

memory; and

a hardware computer processor configured to perform operations comprising:

receiving, from a user computing device of a user, a selection of a third-party entity;

identifying an Application Programming Interface (API) token associated with the third-party entity;

transmitting the API token to a system in electronic communication with the third-party entity;

receiving, via the system, indicators of one or more accounts of the user with the third-party entity;

receiving, from the user computing device, a selection of an account of the one or more accounts;

accessing, via a secure communication session initiated with the API token, a plurality of data items of the selected account of the user with the third-party entity;

transmitting a user interface data to the user computing device, the user interface data configured to depict a user interface on a display of the user computing device, the user interface including one or more interactive elements selectable to indicate authorized uses of the data items by the computing system;

receiving, from the user computing device, a selection of authorized uses of at least a subset of the data items; and

in response to receiving the selection of authorized uses, selectively sharing at least the subset of the data items with a computing device for the one or more authorized uses.

15. The computing system of claim 14, wherein the computing system comprises the system in electronic communication with the third-party entity.

16. The computing system of claim 14, wherein the system in electronic communication with the third-party entity is operated by a third-party.

17. A non-transitory computer readable medium having executable instructions stored thereon, the executable instructions executable by a hardware computer processor to perform operations comprising:

receiving, from a user computing device of a user, a selection of a third-party entity;

identifying an Application Programming Interface (API) token associated with the third-party entity;

transmitting to a system in electronic communication with the third-party entity, the API token;

receiving, via the system, indicators of one or more accounts of the user with the third-party entity;

receiving, from the user computing device, a selection of an account of the one or more accounts;

accessing, via a secure communication session initiated with the API token, a plurality of data items of the selected account of the user with the third-party entity;

transmitting first user interface data to the user computing device, the first user interface data configured to depict a first user interface on a display of the user computing device, the first user interface including one or more interactive elements selectable to indicate authorized uses of the data items by a computing system; 5

receiving, from the user computing device, a selection of authorized uses of at least a subset of the data items; and

in response to receiving the selection of authorized uses, 10
selectively sharing at least the subset of the data items with a computing device for the one or more authorized uses.

18. The non-transitory computer readable medium of claim 17, wherein the operations further comprise: 15
transmitting second user interface data to the user computing device, the second user interface data configured to depict a permissions interface element that is selectable to indicate authorization to access account information associated with the user; and 20

receiving, from the user computing device, authorization to access the account information associated with the user.

19. The non-transitory computer readable medium of claim 17, wherein the operations further comprise: receiving 25
credentials for accessing account information associated with the user at the third-party entity.

20. The non-transitory computer readable medium of claim 17, wherein selectively sharing at least the subset of the data items is with one or more third parties. 30

* * * * *